



**Hewlett Packard
Enterprise**

HPE 3PAR OS 3.2.2 GA/EGA/MU1/MU2/ EMU2/MU3/MU4/EMU4/MU6 Release Notes

Abstract

This document describes the features and issues included in HPE 3PAR OS 3.2.2 GA/EGA/MU1/MU2/EMU2/MU3/MU4/EMU4/MU6 and is intended for use by Hewlett Packard Enterprise customers, partners, and field representatives.

Part Number: QL226-99717a
Published: November 2017
Edition: 1

Notices

© 2014-2017, Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Export of the information contained in this publication may require authorization from the U.S. Department of Commerce.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Contents

3PAR OS 3.2.2 Release Notes.....	6
Online Upgrade Considerations.....	6
Supported Platforms.....	6
End of Support Features.....	6
Components.....	6
What's New in the OS.....	12
Hardware enablement.....	13
Software innovations.....	13
Interoperability.....	16
Modifications to the OS.....	16
Known Issues with the OS.....	25
Modifications to File Persona.....	27
Known Issues with File Persona.....	28
 HPE 3PAR 3.2.2 CLI Release Notes.....	 36
Installation Notes for the CLI.....	36
Supported Operating Systems.....	36
What's New in the CLI.....	36
Removed and Deprecated Commands and Options.....	37
Changed commands.....	37
Modifications to the CLI.....	40
 3PAR OS 3.2.2 CIM API Release Notes.....	 44
What's new with 3PAR CIM API.....	44
Interface changes.....	45
Removed and Deprecated Commands and Options.....	45
Modifications to the 3PAR CIM API.....	45
 3PAR OS 3.2.2 Web Services API Release Notes.....	 47
What's New with the 3PAR Web Services API Software.....	47
Interface Changes.....	48
Modifications to the HPE Web Services API	48
Known Issues.....	49
 3PAR OS 3.2.2 EGA Release Notes.....	 50
Online Upgrade Considerations.....	50
Supported Platforms.....	50
Components.....	50
Modifications to the OS.....	51
What's New in the OS.....	51
Known Issues.....	51
 3PAR OS 3.2.2 MU1 Release Notes.....	 52
Online Upgrade Considerations.....	52

Supported Platforms.....	52
Components.....	52
Modifications to the OS.....	53
What's New in the OS.....	54
Known Issues.....	54
3PAR OS 3.2.2 MU2 Release Notes.....	55
Online Upgrade Considerations.....	55
Customer Self-Upgrade (CSU).....	55
Supported Platforms.....	55
Components.....	55
Modifications to the OS.....	56
What's New in the OS.....	59
Known Issues with the OS.....	60
Modifications to File Persona.....	60
What's New with File Persona.....	62
Known Issues with File Persona.....	62
3PAR OS 3.2.2 MU2 CLI Release Notes.....	64
Installation Notes for the CLI.....	64
Supported Operating Systems.....	64
Modifications to the CLI.....	65
What's New in the CLI.....	65
Known Issues in CLI.....	65
Changed commands.....	66
3PAR OS 3.2.2 MU2 CIM API Release Notes.....	67
Modifications to the CIM API Software.....	67
What's New with the CIM API Software.....	67
3PAR OS 3.2.2 MU2 Web Services API Release Notes.....	68
Modifications to the Web Services API Software.....	68
What's New with the Web Services API Software.....	68
Known Issues.....	69
3PAR OS 3.2.2 EMU2 Release Notes.....	70
Online Upgrade Considerations.....	70
Supported Platforms.....	70
Components.....	70
Modifications to the OS.....	71
3PAR OS 3.2.2 MU3 Release Notes.....	73
Online Upgrade Considerations.....	73
Warnings, Cautions and Notes.....	73
Supported Platforms.....	73
Components Included in this Release	73
HDD/SDD Firmware Included in this Release.....	75
What's New in the OS	76
Modifications to the OS.....	79
Known Issues with the OS.....	85

3PAR OS Patches Included in this Release.....	85
Modifications to File Persona.....	85
Known Issues with File Persona	87
What's New in the CLI.....	87
Modifications to the CLI.....	87
3PAR OS 3.2.2 MU4 Release Notes.....	88
OS Online Upgrade Considerations.....	88
Warnings, Cautions and Notes.....	88
Supported Platforms.....	88
Components Included in 3PAR OS 3.2.2 MU4	88
What's New in the OS.....	90
Modifications to the OS.....	91
Known Issues with the OS.....	94
3PAR OS Patches Included in this Release.....	94
What's New in the CLI.....	95
Modifications to the CLI.....	95
What's New with the CIM API Software.....	95
What's New with the Web Services API Software.....	96
Verification.....	96
3PAR OS 3.2.2 EMU4 Release Notes.....	99
Online Upgrade Considerations.....	99
Supported Platforms.....	99
Components.....	99
Modifications to the OS.....	100
3PAR OS 3.2.2 MU6 Release Notes.....	102
OS Online Upgrade Considerations.....	102
Warnings, Cautions and Notes.....	102
Supported Platforms.....	102
Components Included in 3PAR OS 3.2.2 MU6	102
What's New in the OS.....	104
Modifications to the OS.....	105
Known Issues with the OS.....	109
3PAR OS Patches Included in this Release.....	109
Modifications to the CLI.....	110
Changed Commands.....	110
What's New with the CIM API Software.....	110
Verification.....	111
Support and other resources.....	114
Accessing Hewlett Packard Enterprise Support.....	114
Accessing updates.....	114
Websites.....	115
Customer self repair.....	115
Remote support.....	115
Documentation feedback.....	115

3PAR OS 3.2.2 Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.



CAUTION:

3PAR 3.2.2 EGA Patch 35 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.

Supported Platforms

3PAR OS release supports 3PAR StoreServ Storage. For details, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

End of Support Features

None

Components

Component	Version
OS	3.2.2.290
CLI Client	3.2.2.290
SNMP Agent	1.8.0
File Persona	1.1.1.1-20150828
Drive Cage Firmware:	
DC4 Firmware	2.64
MCU Firmware (OKI)	4.8.28
MCU Firmware (STM)	5.2.49
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	403d
DCS5 / DCS 6 Firmware	1.90

Table Continued

Component	Version
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.05
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x02
Emulex LPe12004 HBA Firmware	02.03.x02
Emulex LPe16002 HBA Firmware	10.4.395.0
Emulex LPe16004 HBA Firmware	10.4.395.0
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

Drive Firmware Details

Type	Capacity	3PAR Drive Model	Speed	Form Factor	3PAR StoreServ Model Supported				Encryption	Firmware
					10000	7000	8000	20000		
FC	300G	HVIPC0300GBFC 15K	15K	3.5"	√					3P04
FC	300G	SEGLE0300GBFC 15K	15K	3.5"	√					3P01
FC	600G	HVIPC0600GBFC 15K	15K	3.5"	√					3P04
FC	600G	SEGLE0600GBFC 15K	15K	3.5"	√					3P01

Table Continued

Type	Capacity	3PAR Drive Model	Speed	Form Factor	3PAR StoreServ Model Supported				Encryption	Firmware
					10000	7000	8000	20000		
SATA	1000G	SMSKP0001TBAT07K	7.2K	3.5"	√					3P01
SATA	2000G	HMRSK0002TBAT07K	7.2K	3.5"	√					3P01
SATA	2000G	HUA722020ALA330	7.2K	3.5"	√					A3GG
SAS	1000G	SAVN1000S5xeN7.2	7.2K	2.5"		√				3P01
SAS	1000G	SAWK1000S5xnE7.2	7.2K	2.5"		√			SED	3P00
SAS	1000G	SAWK1000S5xnN7.2	7.2K	2.5"		√				3P00
SAS	2000G	HMRP2000S5xnN7.2	7.2K	3.5"	√	√				3P00
SAS	2000G	HMRSK2000GBAS07K	7.2K	3.5"	√	√				3P02
SAS	2000G	SAVN2000S5xeN7.2	7.2K	2.5"		√	√	√		3P01
SAS	2000G	SMEG2000S5xnF7.2	7.2K	3.5"	√	√			FIPS	3P00
SAS	2000G	SMEG2000S5xnN7.2	7.2K	3.5"	√	√				3P01
SAS	2000G	SMKR2000S5xeN7.2	7.2K	3.5"	√	√	√	√		3P01
SAS	3000G	HMRP3000S5xnN7.2	7.2K	3.5"		√				3P00
SAS	3000G	HMRSK3000GBAS07K	7.2K	3.5"		√				3P02
SAS	3000G	SMEG3000S5xnN7.2	7.2K	3.5"		√				3P01
SAS	4000G	HMRP4000S5xnN7.2	7.2K	3.5"	√	√				3P00

Table Continued

Type	Capacity	3PAR Drive Model	Speed	Form Factor	3PAR StoreServ Model Supported				Encryption	Firmware
					10000	7000	8000	20000		
SAS	4000G	SMEG4000S5xnF 7.2	7.2K	3.5"	√	√			FIPS	3P00
SAS	4000G	SMEG4000S5xnN 7.2	7.2K	3.5"	√	√				3P01
SAS	4000G	SMKR4000S5xeN 7.2	7.2K	3.5"	√	√	√	√		3P01
SAS	6000G	SMKR6000S5xeF 7.2	7.2K	3.5"		√	√	√	FIPS	3P02
SAS	6000G	SMKR6000S5xeN 7.2	7.2K	3.5"	√	√	√	√		3P01
SAS	300G	HKCF0300S5xeN 015	15K	2.5"	√	√	√	√		3P02
SAS	300G	SYJKT0300GBAS 15K	15K	2.5"	√	√				3P01
SAS	450G	HCBRE0450GBAS 10K	10K	2.5"	√	√				3P02
SAS	450G	SLTN0450S5xnE0 10	10K	2.5"	√	√			SED	3P00
SAS	450G	SLTN0450S5xnF0 10	10K	2.5"	√	√			FIPS	3P00
SAS	450G	SLTN0450S5xnN0 10	10K	2.5"	√	√				3P01
SAS	600G	HCBF0600S5xeN 010	10K	2.5"	√		√	√		3P02
SAS	600G	HKCF0600S5xeF 015	15K	2.5"	√	√	√	√	FIPS	3P02
SAS	600G	HKCF0600S5xeN 015	15K	2.5"	√	√	√	√		3P02
SAS	600G	SLTN0600S5xnN0 10	10K	2.5"		√				3P01
SAS	900G	HCBRE0900GBAS 10K	10K	2.5"	√	√				3P02

Table Continued

Type	Capacity	3PAR Drive Model	Speed	Form Factor	3PAR StoreServ Model Supported				Encryption	Firmware
					10000	7000	8000	20000		
SAS	900G	SLTN0900S5xnE010	10K	2.5"	√	√			SED	3P00
SAS	900G	SLTN0900S5xnF010	10K	2.5"	√	√			FIPS	3P00
SAS	900G	SLTN0900S5xnN010	10K	2.5"	√	√				3P01
SAS	1200G	HCBF1200S5xeF010	10K	2.5"		√	√	√	FIPS	3P02
SAS	1200G	HCBF1200S5xeN010	10K	2.5"	√	√	√	√		3P02
SAS	1200G	HCEP1200S5xnN010	10K	2.5"	√	√				3P00
SAS	1800G	HCBF1800S5xeN010	10K	2.5"	√	√	√	√		3P02
SSD	100G	HRALP0100GBAS SLC	150K	3.5"		√				3P00
SSD	100G	HRALP0100GBAS SLC	150K	2.5"		√				3P00
SSD	100G	HRALP0100GBFC SSD	150K	2.5"	√					3P05
SSD	200G	HRALP0200GBAS SLC	150K	3.5"		√				3P00
SSD	200G	HRALP0200GBAS SLC	150K	2.5"		√				3P00
SSD	200G	HRALP0200GBFC SSD	150K	2.5"	√					3P05
SSD	400G	HRLP0400S5xnE MLC	150K	2.5"	√	√			SED	3P01
SSD	400G	HRLP0400S5xnN MLC	150K	3.5"		√				3P02
SSD	400G	HRLP0400S5xnN MLC	150K	2.5"	√	√				3P02

Table Continued

Type	Capacity	3PAR Drive Model	Speed	Form Factor	3PAR StoreServ Model Supported				Encryption	Firmware
					10000	7000	8000	20000		
SSD	480G	DOPA0480S5xnN MRI	150K	3.5"		√				3P03
SSD	480G	DOPA0480S5xnN MRI	150K	2.5"		√				3P03
SSD	480G	DOPE0480S5xnN MRI	100K	3.5"		√	√	√		3P04
SSD	480G	DOPE0480S5xnN MRI	100K	2.5"		√	√	√		3P04
SSD	480G	HSCP0480S5xnN MRI	150K	3.5"		√				3P02
SSD	480G	HSCP0480S5xnN MRI	150K	2.5"	√	√	√	√		3P02
SSD	480G	HSSC0480S5xnN MRI	150K	3.5"		√				3P02
SSD	480G	HSSC0480S5xnN MRI	150K	2.5"	√	√				3P02
SSD	920G	DOPA0920S5xnN MRI	150K	3.5"		√				3P03
SSD	920G	DOPA0920S5xnN MRI	150K	2.5"		√				3P03
SSD	920G	HSCP0920S5xnF MRI	150K	2.5"	√	√	√	√	FIPS	3P02
SSD	920G	HSCP0920S5xnN MRI	150K	3.5"		√				3P02
SSD	920G	HSCP0920S5xnN MRI	150K	2.5"	√	√				3P02
SSD	920G	HSSC0920S5xnF MRI	150K	2.5"	√	√			FIPS	3P03
SSD	920G	HSSC0920S5xnN MRI	150K	3.5"		√				3P02
SSD	920G	HSSC0920S5xnN MRI	150K	2.5"	√	√				3P02

Table Continued

Type	Capacity	3PAR Drive Model	Speed	Form Factor	3PAR StoreServ Model Supported				Encryption	Firmware
					10000	7000	8000	20000		
SSD	1920G	DOPE1920S5xnN MRI	100K	3.5"		√				3P04
SSD	1920G	DOPE1920S5xnN MRI	100K	2.5"		√	√	√		3P04
SSD	1920G	HSCP1920S5xnF MRI	100K	2.5"	√	√	√	√	FIPS	3P02
SSD	1920G	HSCP1920S5xnN MRI	100K	2.5"	√					3P02
SSD	3840G	DOPM3840S5xnN MRI	100K	2.5"		√	√	√		3P03

What's New in the OS

The new features available in 3PAR OS 3.2.2 address improved service levels and data protection with new support for end-to-end data integrity, availability and protection optimized for flash. 3PAR OS 3.2.2 also addresses the need for quick response with an elastic four-way resource pool that provides simple federated workload balancing.

3PAR OS 3.2.2 includes new and enhanced features in the following areas:

- Support for 3PAR StoreServ 20000 Storage Systems
- Support for 3PAR StoreServ 8000 Storage Systems
- 3PAR StoreServ Management Console 2.2
- Support for Higher Scalability
- Persistent Checksum on 3PAR StoreServ 20000
- Remote Copy Asynchronous Streaming
- Peer Persistence for RHEL
- HPE StoreOnce Recovery Manager Central
- 3PAR File Persona
- Peer Motion Software
- Online Import Software
- Priority Optimization Software
- Adaptive Flash Cache
- iSCSI enhancements
- VMware VVOLs
- Autonomic Rebalance enhancements

- On-node System Reporter changes
- Adaptive Optimization new options
- LDAP improvements
- Smart SAN support

Hardware enablement

3PAR StoreServ 20000 series

The 3PAR StoreServ 20000 Storage family offers enterprise flash arrays ready for massive consolidation of most demanding workloads with greater than 3 million IOPS, sub-millisecond latencies, a 4X density advantage, and scalability to 15 PB of usable capacity. The flash-first architecture features the 3PAR Gen5 Thin Express ASIC for silicon-based hardware acceleration of thin technologies, including inline deduplication to reduce acquisition and operational costs by up to 75% without compromising performance. A choice of models provide a range of options that support true convergence of block and file protocols, all-flash array performance, and the use of SSDs (Solid State Drives) with spinning media for unmatched versatility. Enhanced Tier-1 storage capabilities for always-on data access and fine-grained QoS (Quality of Service) controls ensure predictable service levels for all workload types. Bidirectional data mobility enables virtually limitless elastic pools of storage to support the most rigorous on-demand infrastructure.

3PAR StoreServ 8000 series

3PAR StoreServ 8000 Storage offers enterprise Tier-1 storage at a midrange price. 3PAR StoreServ 8000 Storage delivers the performance advantages of a purpose-built, flash-optimized architecture without compromising resiliency, efficiency, or data mobility. The new 3PAR Gen5 Thin Express ASIC provides silicon-based hardware acceleration of thin technologies, including inline deduplication, to reduce acquisition and operational costs by up to 75% without compromising performance. With unmatched versatility, performance, and density, 3PAR StoreServ 8000 Storage gives you a range of options that support true convergence of block and file protocols, all-flash array performance, and the use of spinning media to further optimize costs. 3PAR StoreServ 8000 Storage offers rich, Tier-1 data services, quad-node resiliency, seamless data mobility between systems, high availability through a complete set of persistent technologies, and simple and efficient data protection with a flat backup to StoreOnce Backup appliances. 3PAR StoreServ 8000 series provides four models to choose from: 8200, 8400, 8440, and 8450. You can start with the entry level model and upgrade easily when required.

Software innovations

3PAR StorServ Management Console 2.2

3PAR SSMC (StoreServ Management Console) is a new management and reporting console that offers converged management of both File and Block on 3PAR StoreServ systems. 3PAR System Reporter is fully integrated in SSMC and offers reporting templates, scheduled reports, and threshold alerts.

Support for higher scalability

3PAR OS 3.2.2 enables higher scalability in terms of maximum numbers of volumes, snapshots and initiators. To know more, see 3PAR support matrix available on the SPOCK website <http://www.hpe.com/storage/spock>

Persistent Checksum on 3PAR StoreServ 20000

3PAR Persistent Checksum powered by 3PAR Gen5 ASIC ensures end-to-end Data Integrity via T-10 DIF (Data Integrity Field) enabled via integration with host HBAs and Hewlett Packard Enterprise drivers. This software provides data checks from the host to 3PAR StoreServ back-end media drives. It eliminates media

and transmission errors caused by any component in the I/O stack and provides end to end protection for all data stored on 3PAR StoreServ Storage systems via a completely agentless and application agnostic solution.

NOTE:

This feature is available only on 3PAR GEN5 ASIC platforms. For a complete list of supported hosts and HBAs, see the SPOCK website <http://www.hpe.com/storage/spock>

3PAR Remote Copy

3PAR Remote Copy Synchronous mode supports extended round trip latency of up to 5 ms using either RCFC, FCIP or RCIP transports.

3PAR Peer Persistence

3PAR Peer Persistence extends the support for Linux Red Hat Enterprise and provides Oracle RAC support on RHEL and Windows Server. For more details, see the SPOCK website <http://www.hpe.com/storage/spock>

StoreOnce Recovery Manager Central 1.1

StoreOnce RMC (Recovery Manager Central) 1.1 integrates 3PAR StoreServ with StoreOnce Backup systems to provide a converged availability and flat backup service for 3PAR or VMware environments that augment traditional backup approaches. Combining the performance of snapshots with the protection of backups, StoreOnce RMC for VMware enables fast, efficient, reliable, and simple one click protection for VMDKs (VMware virtual machine disks) and data stores. Rapid online recovery allows VMware administrators to create hundreds of non-disruptive, application consistent VM (Virtual Machine) snapshots (local or remote or both) and initiate rapid online recovery. This solution provides a 17x faster backup and 5x faster restore of snapshot data with flat backup with RMC's Express Protect feature. This feature enables the flat backup of VM snapshot data from 3PAR to StoreOnce, independent of backup server software.

3PAR File Persona

3PAR File Persona is a licensed feature that enables a rich set of file protocols, file data services, and an Object Access (REST) API. It extends the spectrum of primary storage workloads natively addressed by 3PAR StoreServ Storage systems to include home directories and user shares; content management and collaboration; data preservation and governance; and custom cloud applications. 3PAR OS 3.2.2 doubles the aggregate usable file capacity supported per node pair from 64 TB to 128 TB. Network connectivity is increased to 12 x 10GbE ports per node pair on 3PAR StoreServ 20000 series systems. The on-board RCIP port can be used for file access on all File Persona supported 3PAR StoreServ systems. File storage efficiency is improved with support for Thin Deduplication. Trend Micro ServerProtect for Storage is supported for virus scanning.

Peer Motion Software

Peer Motion Software brings multi-array bidirectional peer motion capabilities across multiple systems. This solution allows customers to optimize the costs by setting up an elastic pool of capacity across any 3PAR StoreServ system—mapping their workload to the right resources and choosing between a midrange, an all flash, or enterprise flash storage system—as the requirements for that workload can change over time. It also provides features such as concurrent migrations, prioritization of migration tasks, and data mobility from multiple sources running legacy 3PAR OS releases to a single destination 3PAR StoreServ system.

Online Import software

Online Import software allows customers to move data from legacy non-3PAR storage to 3PAR StoreServ systems with minimal or no disruption. 3PAR Online Import software provides an easy way to modernize

EVA, EMC VMAX, EMC VNX, VNX2, CLARiiON CX4, and HDS storage infrastructure with a simple migration process. The following HDS platforms are supported:

- HDS TagmaStore NSC
- HDS TagmaStore USP
- HDS USP V
- HDS USP VM
- HDS VSP

3PAR Online Import allows data mobility from multiple source systems to a single destination system in a single configuration. Users can migrate a subset of a volume exported to the host, if they do not wish to migrate the entire host in one go. Migration tasks can be prioritized, and migration of the volumes with the critical data can be assigned a higher priority.

Priority Optimization software

Priority Optimization software enables customer to set latencies goals down to 500 microseconds on all-flash configurations.

Adaptive Flash Cache

Adaptive Flash Cache will now use RAID 0 as a default layout on 3PAR StoreServ 7000, 8000 and 20000 series storage systems.

iSCSI enhancements

3PAR OS 3.2.2 provides the following iSCSI enhancements:

- Support for Persistent Ports loss_sync recovery, automatic failover in case of a failure due to loss of signal or link down between the array and the switch.
- Enhanced SendTarget discovery to return multiple target portals.
- Support for 256 iSCSI initiators (maximum) per port on 3PAR StoreServ 8000 and 20000 Storage systems.
- Support for iSCSI VLAN tagging on 3PAR StoreServ 8000 and 20000 Storage systems.
- Support for Enterprise iSCSI (iSCSI over DCB/lossless Ethernet) on 3PAR StoreServ 8000 and 20000 Storage systems.
- Support for iSCSI IPv6 on 3PAR StoreServ 8000 and 20000 Storage systems.

VMware VVols

VMware VVols support provided in 3PAR OS 3.2.2 enables higher VVols scalability, provides support for multiple storage containers, and provides ability to use the same array with multiple vCenters and vCenter Clusters. With the new command line options, the storage administrator gets more visibility into the capacity and the performance for individual VMs.

Autonomic Rebalance enhancements

Autonomic Rebalance enhancements trigger automatic rebalancing of existing volumes as new drives are added on 3PAR 7200 and 8200 systems. All other classes of system rebalance manually by running the `tunesys` operation. This release provides several optimizations for improving performance of rebalancing activity and reporting of the rebalancing activity.

On-Node System Reporter

On-Node System Reporter provides the ability to grow the size of the .srdata volume to allow longer retention of historical data collections. You can protect .srdata volumes using snapshots via Virtual Copy.

Adaptive Optimization

Adaptive Optimization in 3PAR OS 3.2.2 provides the user more control over the space distribution within AOCFG CPGs. You can define a minimum and maximum space utilization of each tier in an AOCFG. You can also define minimum space utilization of the T0 CPG (SSD tier) such that the SSDs remain mostly full, making full use of the SSD performance.

LDAP improvement

3PAR OS 3.2.2 brings following LDAP improvements:

- Support for multiple LDAP servers — This version allows an unlimited numbers of LDAP servers to be defined.
- Support multiple domains — This version allows any users defined in domains that fall under the same root domain.
- Ability to lookup servers in DNS.
- Load balancer support via a new LDAP-type option.

3PAR Smart SAN

3PAR Smart SAN enables you to automate peer zoning which results in the creation of fewer zones and enables configuration of zones in minutes through its TDPZ (Target Driven Peer Zoning) feature. Through automation, it reduces the probability of errors and potential downtime.

Without 3PAR Smart SAN, an administrator must pre-configure zones on the switch before configuring hosts and VLUNs on the 3PAR StoreServ Storage system. With 3PAR Smart SAN, the administrator can configure and control zoning directly from the 3PAR CLI. 3PAR Smart SAN also supports standards-based device registrations and diagnostics data collection for better configuration visibility and diagnostic purposes.

Interoperability

3PAR OS 3.2.2 is the last major 3PAR OS release to support Host Persona 1 with any version of Citrix XenServer 6. Subsequent 3PAR OS versions will exclusively use Host Persona 2 for any version of Citrix XenServer 6 and later.

Modifications to the OS

The following items are addressed in this release:

Issue ID	Description
49957	If the admin interface is non-functional, an alert is reported but management of other network ports is not affected.
80418	Addresses an issue where an SFP event/alert does not work correctly when the SFP error is cleared.

Table Continued

Issue ID	Description
80428	<p>Resolved an issues where details of a fully provisioned volume split between tiers by Adaptive Optimization might display the wrong RAID type and device type (SSD, FC, NL) information. This also affects the tier from which any new space is allocated to the VV using the <code>growvv</code> command.</p> <hr/> <p>NOTE:</p> <p>Changing the primary CPG for a fully provisioned volume must be done by using the <code>setvv</code> command with options <code>-usr_cpg</code> or <code>-snp_cpg</code>.</p> <hr/>
83509	If repeated attempts to clean a chunklet fail, mark the chunklet as media failed and go on to the next chunklet.
92692	<p>The TOC information for an iSCSI port might become incorrect if an FC adapter is replaced with a CNA adapter. The iSCSI port might intermittently come up in <code>config_wait</code> state following node reboot or node panic. Resetting the port clears the <code>config_wait</code> state.</p> <p>To resolve the inconsistency in the TOC, switch the port to FCoE mode and then switch it back to iSCSI mode.</p>
93554	The user can input multiple DNS addresses when running OOTB (Out-of-the-Box).
94331	Resolved an issue where the 3PAR Management Console Volume Raw Space pie chart on the Physical Disks Summary tab incorrectly displays value on StoreServ with Adaptive Optimization software active.
95780	The <code>updatevv</code> command algorithm is revised so that the structures around the snapshot need not be recreated and chances of losing the snapshot on failures are reduced.
96308	<p>For 3PAR StoreServ 7000 storage systems, the <code>locatecage</code> command turns on the enclosure LED and all the drives LEDs to locate an entire cage. To locate an entire cage for 3PAR StoreServ 20000 storage systems, only the enclosure LED is turned on.</p> <p>The <code>locatecage</code> command requires the <code>-t</code> option which specifies the number of seconds to turn on the LED. For 3PAR StoreServ 7000 storage systems, the default time is 15 minutes with a maximum of 1 hour. For all other systems, the default time is 60 seconds with a maximum of 255 seconds.</p> <p>The <code>jbod_monitor</code> checks this time every 2 minutes if it has elapsed and turns off the LED.</p> <p>To turn off LED before the time has elapsed, use 0 for seconds for the <code>-t</code> option.</p>
98668	Resolved an issue of potential deadlocks while stopping Remote copy function.
99402	The <code>controlport logout</code> command can be run for FCoE ports.
100837	For remote copy traffic, Remote copy links must have a minimum of 5 Mbps throughput available to them.
102997	Low priority rules can only throttle low priority rules, and normal priority rules can only throttle normal and low priority rules.

Table Continued

Issue ID	Description
104176	During system manager startup, cage component state is observed for more time before posting cage component state change alerts for loop being offline.
104239	Support is provided for 10G SFPs for QLogic EP8324.
105680	Using the command <code>controlsr grow <size></code> , it is possible to grow the volume used to store SR data and increase the retention time of all SR data categories such as hires, hourly, daily, and AO ldrq.
106651	Resolved an issue where a region move on a remote node could cause instability.
108365	The system manager synchronization locks are released before making remote procedure calls to the quorum announcer processes. This applies only to Peer Persistence configurations.
108932	LDCK retry speed is enhanced. When ldck failures are added to a retry queue, the whole queue is retried after a period of time instead of just the head of the queue.
109217	If the maximum number of initiators exceeds for a Qlogic CNA port, an alert is raised.
111310	For Windows Peer Persistence support, the recovery procedure must be updated to include a manual disk rescan from Windows Disk Management.
111320	Resolved an issue where local variables in the Quorum Announcer process are overwritten when error message strings from the Quorum Witness are greater than 100 characters in length. When this occurs the Quorum Announcer process restarts.
111321	Releases system manager synchronization locks before making remote procedure calls to the quorum announcer processes. This applies only to Peer Persistence configurations.
112313	During online upgrades, the execution of scheduled tasks is paused. If an upgrade fails during the load phase, the scheduled tasks remain paused even when the system indicates that no upgrade is in progress. This is resolved and the scheduled tasks resume normally if upgrade fails.
112889	Provides support for the <code><n:s:p></code> and <code><wnn></code> options for the <code>servicehost remove</code> command to remove dead connections listed by the <code>servicehost list</code> command.
113074	Provides support for the Subject Alternative Name certificate extension to the certificate handling tools. SANs can be added to CSRs and self-signed certificates with the <code>-SAN</code> option. The <code>showcert</code> command can be used to view the extension.
113301	Resolved an issue where certificate generated by earlier version of 3PAR OS were flagged by OPENSSL as having a unsupported certificate purpose.
113374	The <code>compactcpg</code> command runs automatically.
113514	Temperature Under_Warning_Threshold alerts are changed to informational events.

Table Continued

Issue ID	Description
114460	Resolves an issue where a general protection fault might occur in the SCSI code when running the <code>updatevv</code> command for a VV multiple times in a short period of time.
114947	The volume capacity limit for DR operations is increased to 4096 TB.
115302	When a remote copy volume is undergoing a region move, retry timeout period is 5 minutes. If the volume is not currently involved in a region move, the retry timeout is the default.
115505	The <code>-online</code> option is supported with the <code>creategroupvvcopy</code> command and multiple copies can be created at the same time.
115523	To simplify the configuration and setup of 3PAR systems, the <code>admithw</code> and <code>ootb</code> commands reconfigure the free fibre channel ports to <code>host</code> connection mode and <code>pointconnection</code> type.
116034	When running OOTB (Out-of-the-Box), the user can configure RCIP and File Persona ports.
116685	Added the capability to authenticate with multiple LDAP servers behind a load balancer.
117021	The <code>updatevv</code> command is revised so that the structures, VLUNs and VV sets, around the snapshot need not be recreated and risk of losing the snapshot on failures is reduced.
117892	The default UDID for snapshots is set to VV ID.
118170	Resolved an issues where node shuts down unexpectedly if the <code>controlport</code> <code>cli</code> commands are issued in a particular sequence.
118875	Downgrade to earlier version does not require the on-node System Reporter database to be recreated. Downgrading to earlier versions will still require the re-creation steps in many cases.
119221	An STSG (SendTargets Port Tag) is provided for each iSCSI port. Information of all the ports sharing the same STGT is part of the SendTargets All response.
119332, 126103	The task manager correctly processes all completed tasks regardless of the general load and the AO load on the system. All completed tasks are successfully displayed when the <code>showtask</code> command is issued.
119734	If iSCSI initiators limit is exceeded, an alert is raised.
120838	Space free up operations are made parallel and asynchronous.
120895	Resolved an issue where the <code>checkhealth host</code> commands becomes unresponsive if the SAN provides incomplete data from the port.
121146	Resolved an issues where the failover is not removed correctly if the connection mode of an FC port is changed while a persistent ports failover is active on that port.
121260	By default, the Hyper Threading is disabled.

Table Continued

Issue ID	Description
121830	Resolved a concurrency issue between region mover and <code>nup_post_process_th</code> .
121955	For 3PAR StoreServ 20000 Storage Systems, use the cage info from the SES page to determine the domain of the I/O module and assign the correct LoopA / LoopB port.
122676	Resolved an issue where after a cage reset, drives in an encrypted system remain degraded for a few hours. Now, drives return to the normal state immediately after a cage reset.
122840	Invalid Region Move VL map entries are discovered and automatically removed from the system configuration database. An alert is generated to inform that the situation has been resolved, and events are generated with more specific details.
123901	The dedup garbage collector (ddcscan) is changed so that the master node ddcscan triggers ddcscan runs on other nodes even when there is 1 TB of reuse pages queued up on a node.
124117	Resolves an issue in node up integration that might lead to data unavailability.
124185	The ability to authenticate users in subdomains is provided.
124232	Resolved an issues where single node goes down when recovering meta data on RO snapshot.
124528	Resolved the issues with CPG capacity efficiency displayed by the <code>showcpgr -space</code> command.
124556	Resolved an issue where in certain network environments, it takes more time than the timeout period to configure the network interface making the array inaccessible from an administration standpoint.
124648	Resolved an issue of reclamation of unreferenced space in systems with dedup volumes so that snapshot creation and deletion during such activity does not cause the space reclamation to be abandoned.
125106	Resolves an issue that causes DNS resolution to fail.
125257	Provide a command to trigger the system to update the dedup statistics of any given CPG or TDVV.
125283	The WSAPI startup checks that both parts of the key pair are present and are correct.
125546	After an all nodes down node rescue, select the console option Load network configuration to reload the network configuration.
125733	Provides support for Enterprise iSCSI, iSCSI DCBX information is displayed.
125912	Resolved an issue in DDS space recycle handler that could result in unresponsive system when another thread holds the write lock.

Table Continued

Issue ID	Description
126112	If a power event causes a two node system to go down and a hardware failure prevents one of the nodes from coming back after the power is restored, the system does not start. This is resolved and if the second node does not join the cluster 30 minutes after the first node boot, it proceeds with recovery automatically.
126134	Resolves mismanagement of a token cluster mask that might cause an invalid token consistency check across nodes.
126524	Resolved an issue where if the admin interface changes frequently, the netc process reports an error message due to an unwanted increase in memory usage.
126568	No limitation on the number of LUNs that can be exported to a given host initiator at one time.
126825	The cage firmware image size is increased.
126837	Resolved a SCSI command ID mismatch assert in the FCoE driver.
126987	A new feature is provided to check if ingress and egress DMA operations are within an address range.
127444	Resolved an issue where single node goes down when a region move and I/O operation is going on
127727	P3P firmware is upgraded to 4.15.2.
127849	VASA Provider does not generate an event to notify the vSphere environment if the flash-cache configuration has changed for the VVol storage containers.
128035	When a fully provisioned volume is in an AO configuration, the primary CPG for USR space can be changed to any other AO tier CPG.
128039	The <code>createsv</code> command can be used for creating snapshots of .srdata volume. The <code>promotesv</code> command can be used to promote this snapshot after stopping SR.
128104	Addresses a data integrity issue when migrating virtual machines.
128116, 132299	Resolved an issue where rolling upgrades beyond the 3PAR OS 3.1.3.MU1 fail when preserved data is created during the upgrade.
128178	Default engine ID is used in ContextEngineId field in SNMPv3 scoped PDU.
128243	Support is provided for 10G ethernet port with SFP - AVAGO AFBR-703SDZ-HP1.
128312	Simple LDAP configuration is provided.
129033	Spare chunklets used as the destination for a chunklet move are unmapped after the data is moved.

Table Continued

Issue ID	Description
129674	If less than half of the admitted disks to maintain TOC quorum are present, the <code>setsysmgr</code> command does not start the system.
129818	Resolved an issue where a lack of resources cause host I/O to become unresponsive.
129940	Resolved an issue where completed offline copies cannot resume other operations as the temporary snapshot created is not deleted.
130063, 130654	Resolved an issue where accessing invalid memory address causes <code>snmpagent</code> process failure.
130118	Prior to 3PAR OS 3.2.2, a <code>createsralertcrit</code> criterion could be configured with a name that exceeds 31 characters. When the name exceeded 31 characters, no alerts were reported even if the defined criterion should have flagged the defined condition. To address this issue in 3PAR OS 3.2.2, new <code>createsralertcrit</code> definitions can no longer be created using a name that exceeds 31 characters. Hewlett Packard Enterprise recommends that you verify the length of the name of any existing <code>createsralertcrit</code> definitions. When found, these must be replaced by new <code>createsralertcrit</code> definitions with a name not exceeding this 31 character length limit. Previous definitions must be removed manually.
130663	Both LPe16002 and LPe16004 use two new SFPs from Avago and Finisar Manufacturer : HP-A Part Number : E7Y10A Manufacturer : HP-F Part Number : E7Y10A
130677	Resolved an issue where system manager might become unresponsive when a node battery test starts on an expired battery.
130836	Resolved an issue where the SNMPAgent initialization process fails and a function checking an I/O might encounter a timing issue when a node is shutting down or becoming unavailable
131115	The <code>showcpg -space</code> command displays accurate CPG dedup ratio as data size stored in private space is included in CPG dedup ratio calculation.
131158	Resolved an issue where request for space from L1 bitmap might be incorrect After the volume growth, the data pattern in L1 bitmap page and L2 bitmap reserve area signature might be same. This might cause incorrect result when requesting space from L1 bitmap. This is resolved.

Table Continued

Issue ID	Description
131239	<p>Enhancements to the VASA Provider and VMware VVol support, including:</p> <ul style="list-style-type: none"> • Support for multiple VVol storage containers, including new CLIs to manage them. • Support for migrating from 3PAR OS 3.2.1 based storage containers to the multi-storage container model. <hr/> <p>NOTE:</p> <p>The downgrade from 3PAR OS 3.2.2 to an earlier release is not supported without first removing storage containers.</p> <hr/> <ul style="list-style-type: none"> • Support for connecting multiple vCenters to the VASA provider simultaneously, using the server-side certificate management mode controlled with the <code>setvasa</code> command. • Support and certification for VASA 2.0 as a block device storage provider. • Usability enhancements into several CLIs for viewing VVols
131349	Resolved a condition where 16 Gbps FC driver code might dereference a null pointer when a request to get a node name fails. This can happen during FC link events such as link down, link up, port reset, and so on.
131378	If an SFP not listed in the database is plugged in, it is flagged as not qualified.
131549	Prevents unexpected system manager restarts when moving regions.
132350	Resolved an issue where during node reboots, a <code>ping</code> or <code>statiscsi</code> command might induce an erroneous firmware core on iSCSI ports.
132475	Resolved an issue of SNMPAgent failure due to invalid memory access.
132619	SFP database is updated for 12G SAS connectors.
132644	The internal function to create unique snapshots is modified so that 65K snapshots can be made off of VVs with a similar name.
132748	Resolved an issue where block allocation map for RW snapshots reports incorrect information when data is written to the base VV
132791	Resolved an issue where DCS1 drive cage reports incorrect status.
133245	Resolved an issue where the VASA provider might terminate while updating vSphere trusted certificates.
133457	Resolved an issue where under heavy load, the VASA Provider might abort while performing VVol operations.

Table Continued

Issue ID	Description
133567	The <code>checkhealth</code> and <code>eventlog</code> commands report PDs with FRU or UPG firmware.
133643	Resolved an issue where odd fields are found at the tail of the SNMP trap OIDs which might cause errors for clients when processing incoming traps.
133679	Resolved an issue where <code>rsh</code> command fails to complete during online upgrades to 3PAR OS 3.2.1.MU3 and later.
133844	Support is provided for 10 GB SR SFP+(FCI) for QLE8242
134067	To prevent issues when reading the TOC, the system ensures that the entire TOC area of a PD is readable before admitting the PD.
134292	Resolved an issue with Adaptive Optimization data movement depending on the execution limit.
134481	<p>The VASA provider log file, inside an insplere, could generate incorrect log messages.</p> <p>For example: [Fri May 1 15:33:05 2015].688 session_data.cpp:966: WARN getVVFFromVvolid, getVVCache returned empty for wwn: 60002ac000000000c27ea87b9ebc4033</p> <p>These log messages can be ignored.</p>
134738	SFP verification process does not use HBA serial numbers as it might make SFP disqualified.
134963	<p>The VASA provider logs warning messages as below</p> <p>[Tue May 5 11:52:24 2015].088 https_gw.c:210: WARN Received premature EOF</p> <p>These warnings can be ignored.</p>
134966	<p>Resolved an issue where the VASA Provider generate incorrect log messages in the Insplere such as</p> <p><code>remove_abandoned_trace_files</code> unable to find tracer parent directory.</p>
135072	An alert is generated for 16G FC if the initiator count exceeds the maximum allowed value.
135384	Resolves an issue where certain host SCSI writes to the primary volumes receive good status, instead of a check condition UA, when Remote Copy writes cannot be replicated to the secondary volumes during a Peer Persistence automatic failover.
136536	QLE8362 CNA and QLE2662 FC HBA firmware is updated to version 5.7.3.
136631	The 16 GB adapter port becomes unresponsive, then resets. This issue is resolved in firmware by increasing the high priority firmware task time-out values, as well as introducing software locking mechanisms.
137079	Resolved an issue where registration of the VASA Provider with a vSphere environment might fail if the array has VV set names longer than 24 characters.

Table Continued

Issue ID	Description
137488	Resolved an issue where after rebooting the primary node (node 0) of the array, occasionally the VASA Provider reports Rescan Error in the vCenter Storage Providers status window.
138743	Provided an ability in 3PAR OS 3.2.2 to use an alias to point to multiple LDAP servers in.
138816	If the system shuts down for powerfail save and no disks are visible to the system when it starts up or only a minority of the disks become visible later, it would automatically start despite having less than 60% of the disks available. This could lead to a repeated powerfail save. This is resolved and the system starts only when appropriate.
140869	Resolved a performance issue in the VASA Provider when configurations have several large VLUNs.

Known Issues with the OS

Issue ID	Description
113925	Live migrations of clustered VMs using vFC (virtual Fibre Channel) adapters is not supported in Peer Persistence configurations.
114158	The <code>setlicense</code> command requires a reboot if a license key with HPE SSN serial number is entered.
119997	<p>The time period for which the <code>tunesys -cleanwait</code> command waits for cleaning of the chunklets is half of the time specified by the <code>-cleanwait</code> option.</p> <p>Workaround: Provide twice the expected time delay value to the <code>-cleanwait</code> option. The maximum cleaning delay can be 360 minutes. Provide a value of 720 to get maximum time delay of 360 minutes.</p>
125767	<p>Attempts to upgrade a StoreServ cluster running versions earlier than 3PAR OS 3.2.1 to version later than 3.2.1 might fail.</p> <p>Workaround: The system manager process must be restarted before the upgrade is resumed or retried.</p> <p>To restart the system manager process, issue the following commands from the master node:</p> <pre># setsysmgr quiet_restart # onothernodes killall -9 sysmgr</pre> <p>If the cluster contains more than two nodes, the system manager process on all other nodes must be restarted as well. From the master node, issue the following command:</p> <pre>onothernodes killall -9 sysmgr</pre>

Table Continued

Issue ID	Description
125812	If an attempt is made to tune an SA space LD on a system which has PDs of the target devtype on less than 3 cages on the owner node of the LD, the tune fails. Tuneld assumes that SA space is always RAID 1, set size 3, cage availability.
129428	The <code>statvln</code> command might not work when system has subLUN configured. It returns zero statistics if any wildcard query is used or multiple VLUN IDs are specified.
131304	Regular VV cannot be added to VVol storage container VVset.
131710	All interfaces into the on-node System Reporter reports timeout when requesting large data sets and experience slow performance.
131813	<p>When an incorrect DNS is set using the Service Processor setup wizard, or if the SP and StoreServ initialization is done on a private network with any DNS settings, the SP is unable to establish a CLI connection to the StoreServ and the SP installation process fails.</p> <p>Workaround: To avoid this issue, do not configure DNS using the SP setup wizard; instead, manually configure DNS using the 3PARCUST account after successfully completing the installation:</p> <ol style="list-style-type: none"> 1. In SPOCC, click the SPMAINT tab. 2. Select Option 2 — Network Configuration. 3. Select Option 9 — DNS Configuration. <p>If you configure DNS using the SP setup wizard, you must reinstall the Service Processor software.</p>
138175	<p>Storage vMotion will become unresponsive and timeout if 3PAR OS system manager is restarted while storage vMotion is in progress.</p> <p>Workaround: When Storage vMotion timeouts, verify that 3PAR OS system manager starts successfully by running the <code>showsysmgr</code> command on array, and then initiate storage vMotion again.</p>
138582	The <code>showvvols</code> and <code>showvvols -sc <storage container></code> displays incorrect information on VM in a storage container (VVol datastore) if a VM has one or more virtual disks or RDMS stored in a different storage container.
140288	Downgrade from 3PAR OS 3.2.2 must ensure that RW snapshot is not more than 256. 3PAR OS 3.2.2 supports 2K snapshots.
140776	The 16G Emulex ports do not report the latest SFP information if the port is in a loss_sync state.

Table Continued

Issue ID	Description
141277	vCenter and ESX 6 hosts might intermittently report 0 MB of storage capacity and free space for VVol datastores for a period of up to 20 minutes after 3PAR array node reboot. No user action is required to resolve the issue. vCenter will successfully re-establish full connectivity with the 3PAR VAASA provider and then update the vCenter VVol VASA storage report.
142013	Volumes formatted with the JFS file system cannot be migrated online via Peer Motion. Hosts using the JFS file system must stop the I/O and the file system must be unmounted before proceeding with the migration. JFS2 and other supported AIX file systems do not have any impact.

Modifications to File Persona

Issue ID	Description
54914 (56736, 60558)	Resolved an issue where a file with actual size of 1 KB is reported as 1 MB 'Size on Disk' from an SMB3 clients and 4 KB 'Size on Disk' from SMB2 clients.
56242	Resolved an issue where quotas cannot be deleted if they are set for a deleted user or group.
57316 (57329, 61080)	Resolved an issue where LDAP user authentication fails when some nodes lose the ability to communicate with the LDAP server.
58579	Resolved an issue where if the filesystem get unmounted during an active NDMP backup or restore session, the filesystem goes in FREEZED condition as NDMP is holding file handles from the filesystem.
59013	Resolved an issue where the request to delete an object share might display <code>Request failed</code> message even if the the object share is deleted successfully.
59046	Resolved an issue where if the File Provisioning Group (FPG) names are not specified in correct case when creating or listing shapshots, showsnap displays <code>No shapshots listed</code> message instead of the FPG not found message.
59193 (61173)	Resolved an issue where if the AV scan policy is set to OFF, it might cause unwanted increase in memory leading to node going down and causing failover.
60018 (60047, 60048)	Resolved an issue where deleting and or adding a VFS with the same IP but with two different subnet masks can cause the VFS to enter a degraded state.
60526	Resolved an issue where creating or growing multiple FPGs in parallel might result in an error message.

Table Continued

Issue ID	Description
60681 (60739, 60740)	Resolved an issue where, on some occasions such as the combination of a node failure and failover, SMB firewall ports might not be configured for a FPG upon recovery and prevent user access to shares on that FPG.
60765	Resolved an issue where an offline upgrade from 3.2.1 MU2 with Patch 08 (P08) with File Persona enabled might leave failover in a disabled state and a future failure might not trigger a failover correctly.
61460	Resolved an issue where using unsupported locale settings during file creations might cause problem during file removal operation.
61795	Resolved an issue where an upgrade might fail if an upgrade pre-check is run during the upgrade.
62025	Resolved an issue where under certain SW failure conditions, all FPGs do not fail over successfully to the backup node.
118770	The output of the <code>showfsav pol</code> command is changed to have a single consistent header for the virtual file server and file store sections.
123354	Resolved an issue where file shares might become inaccessible if multiple PDs containing File Persona volume data go offline due to disk drive failures or service operations.
126831	The <code>createfpg</code> CLI command supports the <code>-tdvv</code> option to create FPGs with thin deduplicated virtual volumes.
130873	Resolved an issue where CPG Out of Space condition causes deactivation of FPG.
134044	The <code>setfshare</code> and <code>showfshare</code> commands provide new options such as <code>-acl</code> , <code>-mode</code> , <code>-owner</code> , <code>-group</code> and <code>-dirperm</code> for file share directory permissions management. For more details, see the <i>HPE 3PAR File Persona User Guide</i> .
135466	The role for the commands <code>setfs</code> , <code>setfsuser</code> , <code>setfsgroup</code> , <code>createfsuser</code> , <code>createfsgroup</code> , <code>removefsuser</code> , and <code>removefsgroup</code> is changed to SUPER.

Known Issues with File Persona

NOTE:

The known issues for 3PAR OS 3.2.1 MU3 File persona are still present in 3PAR OS 3.2.2 unless otherwise listed as addressed in 3PAR OS 3.2.2.

Issue ID	Description
37406,37422	SMB and FPG read and write statistics reported in the <code>statfs</code> command do not account for the data transferred via ODX.
42322	3PAR File Persona does not currently support NBNS (NetBIOS Name Server) resolution. The NetBIOS name of a File Persona cluster node cannot be resolved from Windows clients using the <code>nbtstat</code> command. Issuing the <code>nbtstat - A <HP SMB server IP address></code> command from a Windows client returns a <code>host not reachable</code> error.
42454	CIFS connection lost intermittently and new connections are not allowed. Workaround: Set <code>Smb2Enabled</code> parameter value to 0 in the HP-SMB registry and then restart SMB Services.
48696	Overlapping writes to the same file from NFS and SMB might cause corruption.
51093	On failover of multiple FPGs with a combination of SMB and NFS shares with active I/O, you might experience that some FPGs do not failover. Workaround: Execute the <code>setfpg -f -failover <fpg01smb></code> command on the FPG that does not failover on the first attempt.
52678	Unexpected failover of FPGs might occur while running a SPECfs workload and an alert is generated. Workaround: The FPGs must be failed back to their original node with the <code>setfpg -failover</code> command.
54778, 54687	NFS/HTTP users do not have access to the folder if permission is given with built in domain users group. This is a limitation with respect to cross protocol support. For more details, see <i>Setup Guide for HPE 3PAR File Persona in a Cross Protocol Environment</i> .
55128	If an NFS export is configured with more than 31 client IP addresses, NFS exports can not be modified. Workaround: Limit the number of client IPs used with NFS exports to less than 31. Use a subnet range when possible rather than explicitly specifying each IP address.
57072	LDAP groups are not supported within POSIX ACLs. LDAP Users, Active Directory Users and Groups, and Local Users and Groups are supported within POSIX ACLs. LDAP groups are supported for "chgrp".
58601	If the VSD is not up (or <code>VENDOR_TYPE</code> not set), the files are served irrespective of AV unavailable policy. Files must be served as per AV unavailable policy if AV is ON irrespective of whether VSD is responding or not.
59906	On rare occasion, a request to stop file services on a node might result in restarting of file services instead of going to a stopped state. Workaround: Try again to stop file services on that node and it generally succeeds on the second attempt.

Table Continued

Issue ID	Description
58905 (60564)	Windows and Linux NFSv3 use significantly different methods to process permissions. Windows combine access from all of the ACEs on the file to determine if the user has the requested access. In NFSv3, Linux proceeds through a hierarchy and determines the user's permissions from one of the mode bit fields – user, group, or other. In the NFSv3 Linux behavior, it is possible to get inverted priorities – where others have more permissions than the owner. In Windows' ACL implementation, it is not possible to get such an inversion.
60985	Restarting HPE SMB server multiple times in quick succession causes daemon to become unresponsive, if Active Directory cache contains large number of entries. This occurs when the HPE SMB server is stopped while the Active Directory cache is still being loaded.
52552 (61082)	<p>If both NFS and SMB share refer to the same file system path, then <code>mkdir</code> command issued on the NFSv3 mount from client displays error: <code>mkdir: cannot create directory <dir_name> : invalid argument</code>. But, directory is created.</p> <hr/> <p>NOTE:</p> <p>Hewlett Packard Enterprise does not recommend cross protocol access to the same share for Unity version1.</p> <hr/>
43596 (61247)	When user quota is enabled for hard Inode limit on a Roaming profile user, one less file is allowed to be created on the HPE-SMB share, after logging off. Any attempt to write a file further causes <code>No space on the disk</code> error during logoff.
56895 (61253)	<p>If a share of the .admin file store is set up to copy the configuration backup file to the VFS, the restore might fail if that share is still in place and the share conflicts with a share being restored.</p> <p>Workaround: Before attempting a restore, delete all shares. If the issue has already occurred, delete the FPG and try the restore again.</p>
61184	Many NFSv3 clients do not respond to the EJUKEBOX error no 528 correctly.
61706	<p>Only users added to the <code>B-LOCAL_CLUSTER\Administrators</code> group of server can access C\$ share. <code>LOCAL_CLUSTER\Administrator</code> is added to this group, by default.</p> <p>If a server is joined to an AD domain, then <code>Domain Admins</code> group of the AD server gets added to <code>B-LOCAL_CLUSTER\Administrators</code>. Other users must be added to this group to access C\$ share.</p>
61897 (61913)	Setting an access control entry via UID or GID succeeds only if the ID can be properly resolved to a user or group name.
61920	The configuration backup has an added validation checksum to ensure integrity of the configuration during the configuration restore process. Therefore, a configuration backup taken in the 3PAR OS version 3.2.2 is incompatible for restore in the 3PAR OS 3.2.1 MU3. If 3PAR OS is reverted to 3.2.1 MU3, you must create a new configuration backup compatible with that release.

Table Continued

Issue ID	Description
62719 (62722)	<p>While configuring LDAP provider, if passive node has network issue and cannot contact LDAP server, only the active node gets configured. This causes error in the 3PAR CLI report.</p> <p>Workaround: Resolve the passive node networking issue and then reconfigure the LDAP provider.</p>
62799	<p>When a forced failover of an FPG is required, the VVs associated with the FPG are isolated from being used by the node on the source side of the failover. The time required to isolate the volumes is proportional to the number of volumes, with each volume taking around 2 seconds to isolate. For an FPG of maximum size of 32 TB, grown 1 TB at a time, the forced failover time could be extended by more than a minute.</p> <p>Workaround: Grow FPGs in larger increments to minimize the number of volumes in use. Avoid conditions that require a forced failover of the FPG.</p>
62843 (62848)	<p>As nodes in the cluster are in transition, the health monitor indicates an issue with these nodes. After the nodes are back on-line, they are reported as healthy. Acknowledge the alerts after the update or install of the cluster is complete.</p>
62959 (62976)	<p>Invalid Everyone@somedomain ace is not blocked at the input.</p>
63140	<p>File store snapshots are read only. Moving files from a snapshot to the original folder is not supported.</p> <p>Workaround: Use copy operation when recovering files from a snapshot.</p>
63227	<p>Cross protocol directory changes from NFS are not notified in Win2K12 client.</p> <p>Workaround: Refresh the windows explorer and the changes are visible.</p>
63278	<p>Unresolvable SIDs in Windows ACLs might generate errors while copying files using the <code>robocopy</code> command.</p> <p>Workaround: Use Windows advanced properties to remove the SID from the file. The copy will complete successfully after removing SID.</p>
64247	<p>Duplicate users in multiple configured authentication providers is not supported.</p>
63352	<p>If file store quota is deleted, then every time quota configuration changes, user receives the alert message <code>Quota Event:Unable to persist quota limits on Virtual Server <vfs_name> logged to STaTS</code>. But, quota functionality is not affected due to this alert message logged.</p>
63852	<p>When using bond mode 6, if node fs ports are shut down using the <code>controlport fs state down</code> command or the associated Ethernet switch ports are disabled, I/O might become unresponsive for several minutes depending on the ARP cache timeout when the ports are once again enabled.</p> <p>Workaround: If a client is unable to connect to a share after manipulating the network interfaces, use a client OS specific mechanism to purge the relevant entry from the ARP cache. On some OS, this can be done using the <code>arp -d</code> command.</p>

Table Continued

Issue ID	Description
63901	Because of the POSIX nature of the backing file system, groups cannot be the owners of directories or files. This is an expected behavior.
64221 (64223)	<p>During failover with SMB shares and control port changes, SMB shares loose contact and error on server RDRSocketRead.</p> <p>Workaround: All clients must unmount the SMB share and the cluster must leave the AD domain. Reset the node and then cluster can rejoin the AD domain.</p> <p>If Hewlett Packard Enterprise support is performing the repair, a single node can leave and join the AD domain.</p>
64359	When running an on demand or scheduled virus scan of a large set of files, the expected maximum processing rate is 2 million files per day, depending on load.
64610 (64952)	<p>If the new VFS is created and assigned the IP address of the VFS which is temporarily offline, the two VFS conflict over the IP address when the offline VFS is activated. When the IP address of the newly created VFS is changed with the <code>setfsip</code> command, the <code>showfsip</code> command does not indicate any conflict but conflict exists. This usually manifests as a complaint that the address of one of the pair cannot be activated for the one that shows a different one, because it's already in use on a different policy ID (the ID field displayed by the <code>showfsip</code> command) - the one for the other VFS in the affected pair.</p> <p>Workaround: Remove the IP address of the conflicting VFSs using the <code>removefsip</code> command. Create the addresses on the VFSs again with the <code>createfsip</code> command.</p>
65139	<p>If an attempt to modify a VFS IP fails due to a condition such as a duplicate IP address, the modification are rolled back. However, the reconfiguration of shares for the original IP configuration might not complete and shares remain unavailable.</p> <p>Workaround: Failover the FPG to its backup node and then failback the FPG to the original node using the <code>setfpg -failover <fpgrname></code> command.</p>
65346	The directory structure of File Persona share is not visible in windows explorer after system upgrade from Windows 7_64 to SP1.
65289 (65360)	SuSE SLES11 and SLES11 SP1 client do not support NFS4 ACL.
65204 (65441)	If a group name is reused with a different GID, and that group has a quota, the output of the <code>showfsquota</code> command shows the group name only after about an hour.
65779	If TrendMicro is set as AV vendor, it can not be changed or the policy cannot be removed after remote copy from 3PAR OS 3.2.2 to 3PAR OS 3.2.1 MU3.

Table Continued

Issue ID	Description
66152	<p>After upgrade, VTL is not listed.</p> <p>Workaround: Add and discover VTL again after completing the upgrade.</p> <p>To add and discover VTLs/Tapes:</p> <pre>setfsndmp vtl</pre> <p>To list VTL tapes/drives:</p> <pre>showfsndmp -vtl vtldevices</pre> <pre>showfsndmp -vtl vtltapes</pre>
66344	<p>After upgrade, httpd is not running and FPG full event is seen.</p> <p>Workaround: Remove some content from FPG to free some space in FPG. Umount the FPG and mount it again. This recreates apache configurations, start httpd and make object shares accessible.</p>
66713	<p>You might experience very slow login performance with roaming profiles.</p> <p>Workaround: Turn off either Oplocks or SMB Leases.</p>
67131	<p>LDAP is not configured for node added in cluster expansion, or if node is offline when LDAP changed.</p> <p>Workaround: If a node is out of sync with other nodes in the cluster with regard to LDAP configuration, issue the following commands:</p> <ol style="list-style-type: none"> 1. <pre>setfs ldap -passwd ssmssm99 -schema samba -usessl -certcn set-ldap-host.setldap.com -certfile cert.pem 10.10.10.11 cn=Manager,dc=setldap,dc=com dc=setldap,dc=com set-ldap-host</pre> 2. <pre>setfs auth Local ActiveDirectory Ldap</pre>
67576	<p>During a request to failover an FPG, if that request fails during deactivation of the FPG on the original node, the IPs and shares related to that FPG might be left in an unavailable state.</p> <p>Workaround: Retry the failover request with the <code>setfpg</code> command using <code>-forced</code> option.</p> <pre>setfpg -forced -failover <fpg></pre>
67960	<p>NFS shares created on the default .admin File Store are not restored after completion of the <code>restorefsconf</code> command.</p> <p>Workaround: Remove any existing .admin share configured on target node before issuing the <code>restorefsconf</code> command.</p>
68447	<p>In some cases, removing a Virtual Tape Library (VTL) device from the cluster using the <code>setfsndmp vtl -<IP address of the VTL></code> command appears to fail. The tape drive and robot information pertaining to the VTL are removed, but the VTL IP address information is still listed. This can be ignored.</p>

Table Continued

Issue ID	Description
68497, 68597	<p>Unavailability of NFS shares after remote copy with source and target FPGs having same names.</p> <p>Workaround: Do not setup Remote Copy between source and target File Persona Clusters that share duplicate FPG names.</p>
68694	<p>If an incorrect File Persona snap_name is passed to the <code>removefsnap</code> CLI command, it returns error code - 643. This indicates that a non-existent snap name is specified in the command</p>
118467	<p>Under rare circumstances, the <code>startfs</code> command might fail after printing 'Executing "createfsvm fs_cpg"'. An alert is generated which indicates that the <code>createfsvm</code> task has failed.</p> <p>Workaround: Run the <code>startfs</code> command again.</p>
124078	<p>Creating and editing an FPG, VFS, file store or file share with special characters in the comment field can fail or the comment may not be displayed correctly. Error messages include but are not limited to the following:</p> <ul style="list-style-type: none"> Failed: status=500, exception Failed: unmatched open brace in list Failed: list element in braces followed by "\" instead of space FAILED : Command contains unprintable characters: <p>Workaround: Avoid using special characters in comment fields.</p>
128699	<p>File Persona does not support names with only the "-" character. This is prevented in the 3PAR OS CLI for 3.2.2, but is allowed in the GUI.</p> <p>Workaround: Avoid creating File Persona objects with the name "-".</p>
128847	<p>The <code>createsched</code> command has a limit of 127 characters for the command being scheduled. If the combination of the FPG/VFS/FStore names and the tag selected is too long, scheduling of snapshots for File Stores with long paths and tags might not be possible.</p> <p>Workaround: Use shorter names for the FPG/VFS/FStore/Tag, or schedule snapshots using an external client invoking the <code>createfsnap</code> CLI command. (for example, using cron).</p>
133389	<p>File Persona does not support multi-byte characters in the name or description of objects, including FPG, VFS, file store and file share. File share paths created in other tools containing multi-byte characters are shown in the CLI with the string "[international data]".</p>
133596	<p>File Store names containing curly braces { or } can cause SSMC (3PAR StoreServ Mangement Console) to display incorrect information associated with that File Store.</p> <p>Workaround: Avoid creating File Stores with names that contain { or }.</p>

Table Continued

Issue ID	Description
136787	<p>Under scenarios where a significant block workload exists, FPGs (File Provisioning Group) on a controller node might be automatically migrated to the partner node. This can lead to a temporary disruption in client access, depending on the protocols in use. The load on the system must be reduced either through the addition of more hardware (disks/nodes) or by the reduction of client workload. The FPGs must return to their primary node with the use of the <code>setfpg -failover</code> command. For the purposes of this issue, significant block workload is defined as either of the following:</p> <ul style="list-style-type: none"> • VLUN service times of greater than 150 ms, as reported by the <code>statvlun</code> or <code>srstatvlun</code> command • Occurrences of DelAck (delayed acks), as reported by the <code>statcmp</code> or <code>srstatcmp</code> command.
138407	<p>When performing an online upgrade from 3.2.2 to 3.2.2 MU1, some FPGs may failover to the Alternate Node after the upgrade. In that case, you will need to manually fail those FPGs back to the Primary Node for load balancing. Before the upgrade, record the Primary, Alternate and Current Node for each FPG using the "showfpg -d" CLI command or SSMC. Once the upgrade is complete, restore the FPGs to the Primary or previous Current Nodes as needed using the "setfpg -failover" CLI command or SSMC.</p>

HPE 3PAR 3.2.2 CLI Release Notes

Installation Notes for the CLI

Virus Checking

Virus checking is known to slow down and potentially cause issues with installation of the CLI. Before attempting an install or uninstall of the Remote CLI client, shut down all running applications and disable virus-checking software.

Deprecated Commands and Options

The deprecated options for the `cli`, `createuser`, and `setpassword` commands have been removed from the documentation.

Compatibility Changes in this Release

Remote CLI client versions earlier than Remote CLI client 3.2.2 cannot connect to the 3PAR OS, without using `-nosockssl` option.

Compatibility Changes in Next Release

The following options will be removed:

- `cli`: `-pwf`, `-user`, `-password`, and variable `TPDPWFILE`
- `createuser`: `-e`
- `setpassword`: `-save`, `-saveonly`, `-file`

Installation Directory

- **Windows 32-bit:** `C:\Program Files\Hewlett-Packard\HP 3PAR CLI`
- **Windows 64-bit:** `C:\Program Files (x86)\Hewlett-Packard\HP 3PAR CLI`
- **UNIX and Linux:** `/opt/hp_3par_cli`

Supported Operating Systems

For the list of supported operating systems, see the 3PAR CLI Remote Client document on the SPOCK website at <http://www.hpe.com/storage/spock>.

What's New in the CLI

The following new commands are added in 3PAR CLI 3.2.2:

Command	Description
<code>controlsr</code>	Make changes to the System Reporter
<code>controlrecoveryauth</code>	Control the method used to authenticate recovery accounts

Table Continued

Command	Description
setvvols	Create and remove Storage Containers for VVols
showvvols	Show information about VVol storage containers in the system

Removed and Deprecated Commands and Options

The following commands are removed or deprecated in the OS 3.2.1 release.

Removed Commands and Options	
cli -pwf	Replace remote CLI access by ssh access
cli -password	Replace remote CLI access by ssh access
cli -user	Replace remote CLI access by ssh access
controliscsiport dhcp	DHCP is not supported on iSCSI ports.
movepdtospare	use -ovrd instead of -vacate.
setauthparam	use importcert instead of ldap-ssl-cacert.
setpassword -save	Replace remote CLI access by ssh access
setpassword -saveonly	Replace remote CLI access by ssh access
setpassword -file	Replace remote CLI access by ssh access
setsysmgr	-system_ID, -disk_quorum are removed.
srstatqos	Options -vvset and -all_others are deprecated.
tunesys -diskpct	No equivalent command.
setcim	Options -httpport and -httpsport are removed.

Changed commands

Command	Options added (unless stated otherwise)
admithw	-notune
admitpd	-nopatch

Table Continued

Command	Options added (unless stated otherwise)
admitrcopyvv	-noown
controliscsiport	-vlan <vlan_tag>, checkhealth -svc; subcommand:stgt
checkhealth	-svc
createaocfg	-t#min, -t#max
createflashcache	-t
createfpg	-tdvv
createfsshare	-f
creategroupvvcopy	-online, -tdvv, -tpvv, and -snp_cpg
createhost	-port
createsralertcrit	-rpm
createvfs	-tdvv, -full
createvv	-minalloc
createvvcopy	-wwn
histvlun	-p, -vmname, -vmid, -vmhost, -vvolstate, -vvolsc (VVol filters)
histvv	-p, -vmname, -vmid, -vmhost, -vvolstate, -vvolsc (VVol filters)
importvv	-pri, -nocons
locatecage	-t limits changed
movech	-perm functionality change
movepdtospare	-ovrd
removehost	-port
removevlun	-set
setaocfg	-t#min, -t#max
setauthparam	LDAP changes
setclient	matchbulkobjs

Table Continued

Command	Options added (unless stated otherwise)
setcim	-pol one_hwid_per_view
setfsav	-vendor (Trendmicro support)
setfshare	-acl, -mode, -owner, -group
setsralertcrit	-comment, -all, and pattern support
setsys	new parameter: <i>HostDIF DisableDedup</i>
setsysmgr	system_ID and disk_quorum options removed.
setvasa	-certmgmt
setvfs	-certgen
showfshare	-dirperm
showld	-degraded
shownode	-drive displays different result
showport	-iscsivlans
showportdev	subcommand: tzone
showsrr	-ldrg
showsralertcrit	-critical
showvv	-p, -vmname, -vmid, -vmhost, -vvolstate, -vvolsc (VVol filters)
showvvolvm	-binding, -d, -domain, -listcols, -sc [required option], -sp, -showcols, -summary, -p [-vmhost, -vmid, -vmstate], -vv
srhistpd	-rpm
srpdspace	-rpm
srstatpd	-rpm
srstatrcopy	-port
srstatvlun	-port
startao	-t#min, -t#max
statvlun	-p, -vmname, -vmid, -vmhost, -vvolstate, -vvolsc (VVol filters)

Table Continued

Command	Options added (unless stated otherwise)
statvv	-p, -vmname, -vmid, -vmhost, -vvolstate, -vvolsc (VVol filters)
tunesys	-fulldiskpct, -devtype
tunevv	-tdvv, -src_cpg

Modifications to the CLI

Issue ID	Description
18662	All open connections for a given user are removed when that user is removed. When a user's connection is removed, any running commands are aborted. To examine open connections, use the <code>showuserconn</code> command.
25837	A <code>-degraded</code> option is provided in the <code>showld</code> command.
64697	The original location of the chunklet is cleared without actually moving the data in following cases: <ul style="list-style-type: none"> • If <code>-perm</code> option is used on a non-spare chunklet and it is moved to itself • If the destination is left blank and the system chooses a destination on the same disk.
79398	The <code>servicecage remove</code> CLI command is available for users with service privileges.
95593	The alignment of the columns for output of <code>showcage -d</code> command is changed.
97804	The <code>showsrr</code> command provides an option to show LD region samples for user specified time intervals.
100967	A large <code>nodepct</code> value set in the <code>tunesys -nodepct</code> command suppresses inter-node checks and tune generation.
101623	New <code>-pauseduration</code> option is provided for the <code>setsched -suspend</code> and <code>setsched -suspend all</code> command.
102239	Multiple NTP servers can be configured using the <code>setnet ntp</code> command options <code>-add</code> , <code>-remove</code> , and <code>-set</code> .
102813	The <code>tunesys</code> task cancellation might take a long time under some circumstances.
113390	The <code>tunesys</code> PD analysis shows accurate information for the available disks and percentage used for each node.
105155	VVol storage containers (VVol datastores) must be created by the storage administrator. For more details, see the <i>HPE 3PAR VMware ESX/ESXi Implementation Guide</i> .

Table Continued

Issue ID	Description
107758	Resolved an issue where if a tune is performed on a VV which is in an AO configuration, the tune removes all AO optimizations. A check is introduced to warn the user to use <code>-src_cpg</code> option which allows the AO optimizations to be maintained after tuning.
109435	The <code>showsys -space</code> command displays Bulk VVs usage separately.
110417	The <code>-rpm</code> option is provided for the <code>srpdspace</code> , <code>srhistpd</code> , <code>srstatpd</code> , and <code>createsralertcrit</code> commands. The <code>rpm</code> option allows the user to specify the information displayed based on the RPM, the <code>rpm</code> values are 7 (NL), 10 (FC), 15 (FC), 100 (SSD) and 150 (SSD).
114032	Resolved an issue where the CLI help text for the <code>tunesys</code> command shows incorrect default value for the <code>maxchunk</code> option.
114069	A new option is added to the <code>tunesys</code> command to enable rebalancing of a single devtype using intranode tuning.
114528	Using the <code>showvlun -host set:hset</code> command on a system with more than 8K VLUNs might give internal error as follows: Internal CLI error: tableSetWidth line has 8 columns but tableWidth has 6 columns This can occur if the <code>showvlun</code> command is repeated several times in the same session. Add the <code>-t</code> option to the command, <code>showvlun -t -host set:hset</code> .
115747	Resolved an issues where <code>showcage -d</code> command output incorrectly swaps the node cage link speeds for the DP1 and DP2 connectors.
116368	The <code>checkhealth pd</code> command is revised so that it does not report an issue if the columns of a LFF disk cage did not contain all SSD or all HDD disks.
116727	On rare occasions, the remote CLI client on Windows becomes unresponsive when exiting.
116830	The <code>showcage</code> command displays form factor information.
117425	Resolved an issue where the <code>tunesys -f</code> command does not display failed and degraded PDs and spindle count imbalance warnings.
118928	CLI uses the TLS handshake to establish an encrypted socket with the StoreServ. SSL is disabled.
119145	Resolved an issue where the <code>tpdtcl</code> process aborts if the VV names passed to the <code>statvv</code> or <code>histvv</code> commands are separated by commas.
120159	Resolved an issue where the <code>tunevv restart</code> option does not apply to DeDup TDVV volumes.
122872	Resolved an issue where an error failed to link privilege file might occur if many SSH connections are open at the same time.

Table Continued

Issue ID	Description
124315	Resolved an issue where the <code>tuneld</code> command might fail sometimes if the LD region map changes between retrieval and use.
125568	Resolved an issue where use of <code>statvv</code> or <code>histvv</code> commands with VV names longer than 26 characters cause <code>tpdtcl</code> to fail.
125636	Removed the service alert and report in <code>checkhealth</code> about <code>/altroot</code> file system.
126153	Resolved an issue where if large number of tunes are scheduled, <code>tunesys</code> terminates unexpectedly in the internode analysis phase.
126969	While creating new TPVVs, default allocation size can be modified using <code>-minalloc</code> option with the <code>createvv</code> command. Allocation size must be specified in MB.
127082	The <code>createvvcopy</code> command supports <code>-wnn</code> option.
128948	Resolved an issue where the <code>tuneld</code> command reports a failure condition for a tune if it needs to retry some region moves.
128984	Resolved an issue where the intra node tuning phase of <code>tunesys</code> might terminate if it encounters an LD with a malformed creation pattern <code>(-p)</code> string.
130625	The optional <code>sysid</code> argument to <code>setsysmgr wipe</code> is removed as it is not required with 10 digit serial number.
130888	Resolved an issue where if a volume is included in more than one volume sets, Flash Cache policy of the volume might not display enabled state if one of the volume sets is not Flash Cache enabled.

Table Continued

Issue ID	Description																								
131533	<p>To remove a bulkvv or to remove a bulkvv from a VVol storage container VVset, use the <code>-matchbulkobjs</code> option with the <code>removevv</code> command.</p> <hr/> <p>NOTE:</p> <p>To prevent vSphere configuration integrity issues, use the vSphere environment to remove the associated VMs. To remove a vSphere VVol storage container from the array, see the <code>setvvols</code> command. Do not remove individual VVols from the array.</p> <hr/>																								
137344	<p>With the introduction of File Persona, use the adjusted memory sizes shown below to compute the number of available tpdctl connections:</p> <table><tr><th>Adjusted Memory Size</th><th>Total</th><th>Connections</th></tr><tr><td>4 GiB or lower (prior to 3PAR OS 3.1.2)</td><td>64</td><td>16</td></tr><tr><td>8 GiB</td><td>96</td><td>24</td></tr><tr><td>16 GiB</td><td>128</td><td>32</td></tr><tr><td>24 GiB</td><td>160</td><td>40</td></tr><tr><td>32 GiB</td><td>192</td><td>48</td></tr><tr><td>48 GiB</td><td>240</td><td>60 (New)</td></tr><tr><td>>56 GiB</td><td>256</td><td>64</td></tr></table>	Adjusted Memory Size	Total	Connections	4 GiB or lower (prior to 3PAR OS 3.1.2)	64	16	8 GiB	96	24	16 GiB	128	32	24 GiB	160	40	32 GiB	192	48	48 GiB	240	60 (New)	>56 GiB	256	64
Adjusted Memory Size	Total	Connections																							
4 GiB or lower (prior to 3PAR OS 3.1.2)	64	16																							
8 GiB	96	24																							
16 GiB	128	32																							
24 GiB	160	40																							
32 GiB	192	48																							
48 GiB	240	60 (New)																							
>56 GiB	256	64																							

3PAR OS 3.2.2 CIM API Release Notes

What's new with 3PAR CIM API

- Support for 3PAR StoreServ 20000 Storage Systems
- Support for 3PAR StoreServ 8000 Storage Systems
- Replication Services
 - New remote Replication Services indications:
 - Lifecycle indications for rcopy group and volume:
 - TPD_RemoteGroupSynchronizedInstCreation
 - TPD_RemoteGroupSynchronizedInstDeletion
 - TPD_StorageSynchronizedInstCreation
 - TPD_StorageSynchronizedInstDeletion
 - TPD_RemoteGroupSynchronizedInstModification
(CopyState and ProgressStatus changes only)
 - Alert indications for rcopy group and volume up/down:
 - TPD_RemoteGroupSynchronizedCopyStateAlert
 - TPD_StorageSynchronizedCopyStateAlert
 - TPD_RemoteGroupSynchronizedCopyStateClear
 - TPD_StorageSynchronizedCopyStateClear
 - Added capability to
CreateGroupReplicaFromElements
in ReplicationService class to create Async Streaming remote copy group. This is done by specifying the DesiredRPO value within the
ReplicationSettingData
parameter. Depending on the value set for this parameter, either an async streaming or periodic mode rcopygroup is created. For details, see
3.2.2 CIM API Programming Guide
.
- Block Services
 - Added vendor extension extrinsic method
TPD_EnumerateVMWareVolumes

in
TPD_StorageConfigurationService
to enumerate VVols (VMWare Volume).

Interface changes

None

Removed and Deprecated Commands and Options

The
-httpport
and
-httpsport
options for the
setcim
CLI command are removed.

Modifications to the 3PAR CIM API

Issue ID	Description
110819	The -httpport and -httpsport options for the setcim CLI command are removed. The StoreServ blocks all connections to TCP/UDP ports with non-default values.
112588	The SMI-S cimserver ReplicationServices function CreateGroupReplica is corrected for the SyncType Clone as follows: <ol style="list-style-type: none">1. Check if the group specified via the <i>TargetGroup</i> parameter is in the same domain as the SourceGroup.2. If no TargetGroup is specified, create a new group in the same domain as the SourceGroup. The name of the newgroup is taken from the <i>RelationshipName</i> parameter, or the ElementName in the <i>TargetSettingGoal</i> parameter, or is automatically generated.
114238	Async streaming and Recovery Point Objective support is added to CIMServer Replication Services.
120225	The SMI-S cimserver function ReplicationServices::GetPeerSystems is corrected to return the World Wide Name (WWN) of systems that are only reachable via RCIP connections.

Table Continued

Issue ID	Description
121825	Resolved an issue where no StorageVolume instances are returned if a client specifies an empty value for PropertyList in the Associator request of a volume-related CIM_ConcreteJob.
127861	The CreateGroupReplicaFromElements function uses the -nowwn option of the admitrcopyvv command when it adds volumes a newly created Rcopy group.
128205	TPD_DiskDrive.OtherOperationalStatus now supports the value 12 indicating a "degraded" state.
133791	The SMI-S cimserver is updated with a StorageSetting that allows creation of TDVV volumes with TPD_StorageConfigurationService::CreateOrModifyElementFromStoragePool (). The StorageSetting is defined for SSD based DynamicStoragePools. The TPD_ReplicationService::CreateGroupReplicaFromElements() and CreateElementReplica() Clone operations are improved to create TDVV clones.
135327	Duplicate TPD_LUNStatisticalData instances are no longer reported for different VLUNs. The instance iproperty StatisticTime is also now supported.
135667	The extrinsic method TPD_StorageConfigurationService::TPD_EnumerateVMWareVolumes is added which returns an embedded list of VMware bulk VVs. The optional filter parameter is a comma separated list: name=name1 name2 ... vvolstate=<bound unbound> vmid=id1 id2 ... vmhost=host1 host2 .. vvolsc=vvset1 vvset2 ... vmname=vmnam1 vmnam2 ...
138472	Resolved an issue where cimserver process may get into a situation in which a thread servicing a request becomes unresponsive while holding on to a mutex lock, thus making other threads that are trying to service subsequent requests to line up in queue.
140441	CIMserver reports Async Streaming enablement and RPO value for Async Groups.

3PAR OS 3.2.2 Web Services API Release Notes

What's New with the 3PAR Web Services API Software

- Support for 3PAR StoreServ 20000 Storage Systems
- Support for 3PAR StoreServ 8000 Storage Systems
- Added support for the following on-node System Reporter metrics:
 - physicaldiskstatistics
 - physicaldiskcapacity
 - physicaldiskspacedata
 - volumespacedata
 - cpgspacedata
 - vlunstatistics
 - portstatistics
 - cachememorystatistics
 - cpgstatistics – actually logical disk statistics pertaining to a CPG.
- Added support for GET of AO configurations and volume space distribution (equivalent to showvvcpg)
- Added support for configuring async streaming mode
- Added support for creating snapshots off rcopy volumes
- Added license information to system object
- Added support for creategroupsv and updatevv
- Added support for system parameter GET and PUT:
 - remoteSyslog
 - remoteSyslogHost
 - portFailoverEnabled
 - failoverMatchedSet
 - allowWrtbackSingleNode (GET only)
 - allowWrtbackUpgrade (GET only)
 - disableDedup (GET only)

Interface Changes

None

Modifications to the HPE Web Services API

Issue ID	Description
117675	Resolved an issue in WSAPI where it leaks file descriptor if it fails to connect to the WSAPI socket on another node due to node failure.
123431	Resolved an issue where certain characters like '[' are rejected when setting volume objectKeyValue via WSAPI.
124935	Host persona can be queried by the OS assigned ID and filtered by WSAPI assigned ID. The link to the host persona query by the WSAPI assigned ID is added to the result of the host query.
125889	Resolved an issue where communication with WSAPI server using IPv6 address of the array fails
126230	POST and DELETE of /remotecopygroup/volumes map to admitrcopyvv and dismissrcopyvv commands respectively: POST /remotecopygroup/<rcgroup name>/volumes DELETE /remotecopygroup/<rcgroup name>/volumes/<vv name>
126233	Added WSAPI support for system reporter for physical disk, port, VLUN, CPG, CMP statistic and physical disk, CPG, volume space information.
126234	New iSCSI port fields SendTarget and VLAN are added to ports object.
126490	AO configuration support is added to WSAPI.
126491	WSAPI supports the GET operation on following: <ul style="list-style-type: none">• /v1/remotecopygroups/<groupname>/targets• /v1/remotecopygroups/<groupname>/targets/<targetname>• /v1/remotecopygroups/<groupname>/volumes• /v1/remotecopygroups/<groupname>/volumes/<volumename>
137036	A flag is added to cpg object to indicate whether it is deduplication capable.
139321	Resolved an issue where updating comment for volumeset or hostset via PUT fails.
140426	A Boolean flag is added in /remotecopy to indicate if the system supports async streaming mode.

Known Issues

Issue ID	Description
106458	Certain values are not included in response from GET /cpgs if they are default values.

3PAR OS 3.2.2 EGA Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 EGA Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.



CAUTION:

3PAR 3.2.2 EGA Patch 35 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.

Supported Platforms

3PAR OS release supports 3PAR StoreServ Storage. For details, see the SPOCK website at <http://www.hpe.com/storage/spock>.

Components

Component	Version
OS	3.2.2.290 GA+P03
CLI Client	3.2.2.290
SNMP Agent	1.8.0
File Persona	1.1.1.1-20150828
Drive Cage Firmware:	
DC4 Firmware	2.64
MCU Firmware (OKI)	4.8.28
MCU Firmware (STM)	5.2.49
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	403d
DCS5 / DCS 6 Firmware	1.90
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.05

Table Continued

Component	Version
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x02
Emulex LPe12004 HBA Firmware	02.03.x02
Emulex LPe16002 HBA Firmware	10.4.395.0
Emulex LPe16004 HBA Firmware	10.4.395.0
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

Modifications to the OS

3PAR OS 3.2.2 Extended General Availability (EGA) includes the following modifications:

- The recovery time is reduced in cases of unexpected node restarts on 3PAR StoreServ 8000/20000 Storage systems.
- Fixed 3PAR StoreServ 20000 port ordering.

What's New in the OS

3PAR OS 3.2.2 EGA provides all the benefits provided by 3PAR OS 3.2.2 GA and includes the following revision:

The CLI command `showversion -a -b` now displays Drive Firmware and Firmware Database as version numbers.

Known Issues

3PAR OS 3.2.2 EGA includes the following known issue:

LPe1600x FW may be displayed incorrectly by **showport -i** and **shownode -pci** CLI commands.

3PAR OS 3.2.2 MU1 Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 EGA MU1 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.

CAUTION:

- 3PAR 3.2.2 EGA Patch 35 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.
- 3PAR 3.2.2 MU1 Patch 37 must be installed prior to upgrading from 3PAR 3.2.2 MU1 to a later version.

Supported Platforms

3PAR OS release supports 3PAR StoreServ Storage. For details, see the SPOCK website at <http://www.hpe.com/storage/spock>.

Components

Component	Version
OS	3.2.2.326
CLI Client	3.2.2.326
SNMP Agent	1.8.0
File Persona	1.1.1.1-20150828
Drive Cage Firmware:	
DC4 Firmware	2.64
MCU Firmware (OKI)	4.8.28
MCU Firmware (STM)	5.2.50
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	403d
DCS5 / DCS 6 Firmware	1.90
HBA Firmware:	

Table Continued

Component	Version
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.05
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x02
Emulex LPe12004 HBA Firmware	02.03.x02
Emulex LPe16002 HBA Firmware	10.4.395.0
Emulex LPe16004 HBA Firmware	10.4.395.0
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

Modifications to the OS

3PAR OS 3.2.2 MU1 includes the following modifications:

Issue ID	Description
147602	Systems with encryption enabled failed to boot after an offline upgrades from 3.1.3 to 3.2.2 because encryption status could not be determined.
145786	Avoids an unexpected remote controller node restart for large I/Os (>16MB) when using RCFC.
144703	Avoids scenario where conversions will prevent the system from starting after trying to convert a TPVV not aligned on 256 MB.
144921	Avoids an unexpected cluster restart due to excessive consumption of resources.
145163	The Certificate Signing Requests (CSR) being generated by the array did not initialize the CSR version number. This prevent Windows CAs from signing the arrays CSRs. This issue has now been resolved.

Table Continued

Issue ID	Description
116362	During 3PAR OS upgrades, on very rare occasions, the update of NEMOE may be unsuccessful and leave the system with mismatched NEMOE versions. This is now corrected.
149340	The existing 16G driver supports up to 4MB I/O size. The issue is resolved by rejecting any I/O requests above 4 MB, because above 4 MB causes a hung firmware.
148359	When a new virtual volume (VV) is added to the VVSET, if there are any host definitions in the system with an inactive Logical Unit Number (LUN) path, it results in a system manager core. Only check the inactive LUN path that is related to the VVSET to which the new VV is added. If there is an inactive LUN path related to this VVSET, an error is returned due to checking for 90099.
149461	3PAR OS 3.2.2 incorrectly allows the premium mode to be set to an AOCFG object, but it will not allow AO scheduled tasks with premium mode. The functionality was removed but the setting was not.

What's New in the OS

3PAR OS 3.2.2 MU1 provides all the benefits provided by 3PAR OS 3.2.2 EGA.

Known Issues

3PAR OS 3.2.2 MU1 includes all known issues from 3PAR OS 3.2.2 EGA.

3PAR OS 3.2.2 MU2 Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 MU2 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.

CAUTION:

- 3PAR 3.2.2 EGA Patch 35 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.
- 3PAR 3.2.2 MU1 Patch 37 must be installed prior to upgrading from 3PAR 3.2.2 MU1 to a later version.

Customer Self-Upgrade (CSU)

With the release of 3PAR OS 3.2.2 and SP 4.4, StoreServ 7000 and 8000 customers have the option of self-upgrades for 3PAR OS software. If the StoreServ 7000 or 8000 storage system is on 3PAR OS 3.2.2 and SP 4.4, you can self-upgrade the system with any future OS and SP releases. There are different methods to upgrade the 3PAR OS and SP software. Hewlett Packard Enterprise recommends to use the SPOCC GUI that is included within the 3PAR SP. A new full-featured upgrade wizard included in the SP software guides you through the software upgrade process for the 3PAR OS and SP.

Supported Platforms

For details of supported HPE 3PAR StoreServ Storage, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

More information

<http://www.hpe.com/storage/spock>

Components

Component	Version
OS	3.2.2.390
CLI Client	3.2.2.390 ¹
SNMP Agent	1.8.0
File Persona	1.2.0.54-20160113
Drive Cage Firmware:	

Table Continued

Component	Version
DC4 Firmware	2.64
MCU Firmware (OKI)	4.8.28
MCU Firmware (STM)	5.2.52
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	4044
DCS5 / DCS 6 Firmware	1.90
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.06
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x02
Emulex LPe12004 HBA Firmware	02.03.x02
Emulex LPe16002 HBA Firmware	10.6.296.0
Emulex LPe16004 HBA Firmware	10.4.395.0
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

¹ This version of the Linux CLI Client cannot connect to 3PAR arrays running older versions of 3PAR OS including 3.2.2 MU1 and 3.2.2 GA. Use the Linux client from 3.2.2 MU1 (3.2.2.326) or 3.2.2 GA (3.2.2.290) instead. Those can connect to arrays running 3.2.2 MU2, as well as older releases.

Modifications to the OS

3PAR OS 3.2.2 MU2 includes the following modifications:

Issue ID	Description
102537	Adds a safeguard to ensure a consistent Physical Copy from a thinly provisioned source to an existing volume.
113857	Corrects an issue which prevented the BIOS from being properly flashed during a 3PAR OS upgrade.
121029	Alters the collection algorithm to be initiated differently to improve SAS I/O controller file collection success rate.
122710	Corrects an issue in which two nodes could simultaneously become the network master, preventing the array from being managed.
124360	Drive enclosure firmware improved.
124556	Improves network fail-over reliability for the administrative interface.
106217, 125677	Corrects an issue in some customer configurations in which certain I/O inefficacy patterns have resulted in conditions where physical disks became inaccessible through one disk port (DP1, DP2) on a given node.
132139	Prevents a situation where the loss of the controller node currently supplying the administrative network interface can result in that interface remaining inaccessible.
134267	Deduplication GC generates write-same-zero requests for releasing garbage. These zero dirty pages are now returned to the clean queue after cleaning the associated resources and before sending to logical disk (LD) layer.
134711	Addresses an issue that required HP-UX hosts to rescan to find LUNs used for booting from the array.
137878	Corrects an issue in which, when using certain iSCSI adapters on the initiator side with TCP Timestamp option enabled, header alignment issues affect performance.
142643	Ensures that the volume retains its target port group ID (TPGID) in new groups; after Peer Persistence (PP) switchover.
142759	The array initialization process now correctly displays PD state information.
144921	Prevents excessive system calls when certain TCL processes start or exit.
145574	For 3PAR StoreServ 20000 platforms only, when using the HP560SFP+ HBA, port numbering will now be top-to-bottom, as is the standard convention. For StoreServ 7000 and 8000 platforms, which have horizontal HBAs, the port numbering will remain unchanged.
145693	Removes a slow increase in memory usage caused by processing Report Target Port Group (RTPG) commands on the Protocol Endpoint (PE) LUN, which is automatically exported for VMware persona.
146531	Prevents an unexpected node restart by allowing the Fibre Channel (FC) driver to correctly recover from an unsuccessful operation.

Table Continued

Issue ID	Description
146577	<code>showportdev fcfabric</code> command now returns all the devices in the fabric and not limit it to the first 256 members.
146623	Dirty cache buffers are freed after an unsuccessful write to Peer Motion volumes.
147249	The metadata stored in the TOC now has additional logging to aid in analysis.
147603	Prevents host I/O disruption when deleting large Remote Copy snapshots.
147804	Forces the use of the Adaptive Flash Cache (AFC) LDs table of contents (TOC) owner when defining the resources of the LD on the nodes.
148036	Prevents I/Os stalls on the backend of the array, which ultimately results in an unexpected restart of a controller node, by ensuring memory resources are properly freed.
148518	Resolves an issue in which, under certain conditions, node level tuning (<code>tunenodech</code>) may result in excessive disk space usage.
148706	Control pages are now sent to the cage only once to turn off cage and drive LEDs after the <code>locatecage</code> time expires.
149055	Added in <code>-ha</code> argument to grow arguments to allow for the grow to work on 2 cage systems.
149174	The <code>setrcopygroup restore</code> command now reverts to using the <code>-nosync -nostart</code> options.
150221	Extended copy SCSI commands are now aborted if the source LUN is a Remote Copy secondary volume and if the Remote Copy replication direction changes during the extended copy processing.
150289	Detects an invalid originator exchange id (0xffff) used by a remote initiator port in an unsolicited <code>fc4</code> command and handle these as unsupported requests.
150719	Eliminates transient power supply error conditions when communicating with the controller node power supply.
150736	Corrects an issue in which the cache availability percentage calculation based on battery life results in an alert stating the cache is degraded.
151221	Corrects an issue that may cause host I/Os to be unsuccessful during a Peer Motion import operation's completion. The host I/Os are unsuccessful due to volumes entering a preserved state while migrating volumes for clustered operating systems using SCSI-3 reservations.
151237	Resolves an issue in which, if a snapshot tree is currently syncing a remote copy snapshot, <code>updatevv</code> returns an error.
151611	All timezone values are now recognized by the time conversion routines used in the checkupgrade prechecks, upgradechecks and postchecks that are run during OS upgrades.

Table Continued

Issue ID	Description
152328	Corrects an issue in which the cimserver may exit abnormally when attempting to get an instance of a TPD_VolumeSetting for a legacy volume with no usable space.
152554	Automatic Deduplication Store (DDS) defragmentation is seen for DDS of type TDVV2.
152555	Improvements to the power supply signal monitoring prevent an unexpected controller node restart while performing power supply maintenance on the 3PAR StoreServ 20000 array.
152900	Corrects QLIS driver mailbox synchronization issues.
152961	16 GB array driver for all 3PAR platforms now supports maximum I/O sizes of 16 MB instead of 4 MB.
153729	Bypasses false events indicating "Unable to do I/O to the node drive hw_node_ide".
153769	Issue resolved with memory allocation during inquiry processing.
153931	Limited the number of user initiated deduplication space update process based on system memory of each platform, added a service alert if deduplication garbage collection run exceeds reasonable time threshold, and added support to allow dvar (Ddcscan variables) to be set.
154099	During powerfail recovery, DDS is marked pending if any Deduplication Client (DDC) aren't closed. Some DDC that aren't closed are appended to DDS's list, preventing DDS to close properly. This issue is corrected and all pending DDC now close.
154469	Corrects an unexpected controller node restart issue after unexpected system manager restart during conversions.
154489	HPE Inform OS now rechecks the critical faults reported by the PS and fan units.
154387	Pinned data no longer causes controller node issues on all-SSD arrays.
154837	Prevents memory compromise on a cluster configured with AFC simulation mode if the system manager is restarted or unexpectedly restarts and during OS upgrades.
155429	Minimizes impact of memory usage in the VASA provider.
160725	Addresses an issue of some of existing VVs disconnecting when a VV is added to VVset in a multiple-host scenario.
152269	See HPE Security Bulletin HPSBST03586 rev.1.
152388	Prevents an unexpected array restart due to a single controller node restart such as, but not limited to, maintenance activities or online upgrades on systems running 3PAR 3.2.2 MU1. This unexpected array restart affects systems on which Remote Copy was ever configured.

What's New in the OS

3PAR OS 3.2.2 MU2 provides all the benefits provided by 3PAR OS 3.2.2 MU1 and includes the following revisions:

- 16 Gb FC Direct Connect support for all 3PAR platforms; StoreServ 7000, 8000, 10000 and 20000
- Express layout (for SSD only)
- TDVV Scale increase
- Peer Persistence Scale increase
- Online Import for IBM XIV
- 16 GB array driver for all 3PAR platforms now supports maximum I/O sizes of 16 MB instead of 4 MB, starting with 3.2.2 MU2
- 3PAR Remote Copy provides solution for remote replication that enables flexible business continuity. 3PAR Remote Copy Asynchronous Streaming is a new remote replication mode, along with the existing Synchronous and Periodic Asynchronous modes. This mode eliminates the compromise between performance and the level of data protection. 3PAR Remote Copy Asynchronous Streaming helps the customer easily execute a data protection plan that includes a minimal RPO and protect data for replication distances up to 10ms round trip latency.

NOTE:

Contact your Hewlett Packard Enterprise account representative to review the requirements for enabling the 3PAR Remote Copy Asynchronous Streaming feature.

Known Issues with the OS

Issue ID	Description
123082	Once a VMware storage policy has been assigned to a newly created VVol-based VM, it can't be changed using the vSphere interface. VVol storage policies (such as the CPG) can be changed by migrating the VM to a different datastore, and then migrating back, with a new storage policy.

Modifications to File Persona

Issue ID	Description
51218	Only <code>chmod</code> , <code>chown</code> , <code>chgrp</code> , and <code>ls</code> are elevated to super user privileges with the local Administrator account. To perform other operations like <code>rmdir</code> on files where the administrator does not have sufficient access, a command should first be issued to <code>chown/chgrp/chmod</code> the object and then operate on it. This issue is corrected.
52463	There is an internal cache in one of the system processes that runs out of space after 16 FPGs have been created. The process will be automatically restarted and no manual corrective action is required.
52700	This scenario can occur if the nodes are attached to only a single switch and the switch goes down. It can occur in other scenarios in which all network links on a backup node are down at the time a failover is being processed. Once the network links are back up, the corrective action is to use the <code>setfpg -failover</code> command to bring the FPG command back to its proper owner.

Table Continued

Issue ID	Description
52850	If some file persona nodes are stuck "Starting" after a system shutdown or after <code>stopfs</code> for all nodes, the FPGs associated with the down node will not be automatically migrated to the backup node. The FPGs should be migrated with the <code>setfpg -failover</code> command.
53438	Corrects folder recovery issue in which folders are stranded because due to invalid GIDs.
53582	Corrects an issue in which creating an SMB share of an existing directory overwrites the existing permissions, causing potential DU on other protocols' clients.
53637	Before changing the MTU, all FPGs should be deactivated. After the MTU change, they can then be reactivated.
53640	HP-SMB space replacement character for user and group names.
53649	Unexpected failover of FPGs may occur while running a SPECfs workload. If this occurs, an alert will be generated, and the FPGs should be failed back to their original node with the <code>setfpg -failover</code> command. This issue is corrected.
53716	After creating a share directory, you need to create an export with <code>no_root_squash</code> , mount as root, and use <code>chmod/chown/chgrp</code> to modify permissions to something less restrictive. This <code>no_root_squash</code> export can be created with an allowed IP list of a single client to reduce any security impact.
55879	Corrects an issue in which NFS shares were unable to be restored.
56683	Corrects an issues in which, if one wants to rename a file where the characters in the file name only differ in case (e,g file.txt to FILE.txt), then one needs to rename the file in a two-step process 1. Rename file.txt temp 2. Rename temp FILE.txt. Note that SMB is case insensitive but case preserving so the file "file.txt" is the same as "File.TXT".
56685	This condition might likely occur either during boot time, if for example a switch is down, or during failover time. After the link comes up, if the VFS IP is not pingable, the FPGs should be manually deactivated and reactivated using <code>setfpg -deactivate</code> and <code>setfpg -activate</code> or failed over to the partner node with <code>setfpg -failover</code> . Either of these approaches will cause a retry of the network activation, which can now succeed if the link is up.
57056	File Persona settings outside of the Virtual File Server are properly restored in a bare metal scenario.
57057	User flow for modifying the provider stacking order is corrected.
63175	The <code>signingenabled</code> and <code>signingrequired</code> options in <code>setfs smb</code> and <code>showfs -smb</code> now relate to the connection between a client and the 3PAR File Persona. They formerly were controlling the connection between the 3PAR File Persona and the AD server.

Table Continued

Issue ID	Description
68603	Corrects an issue in which File Persona FPG limit is 16 FPGs per StoreServ controller node pair. FPG counts beyond this are not supported.
68615	Addresses HP-SMB service stuck during continuous restarts while working with large AD infrastructure.
72784	Corrects an issue in which the error message "Internal Error" displays when trying to mount FPG with ODV 12.0 on 1.1 software after remote copy.
74770	Customers exceeding the number of tree connects get "Not enough resources" error message. This issue is corrected.
75818, 75820	In some cases, removing a Virtual Tape Library (VTL) device from the cluster using the <code>setfsndmp vtl -<IP address of the VTL></code> command appears indicate that the tape drive and robot information pertaining to the VTL are removed, but the VTL IP address information is still listed. This can be ignored.

What's New with File Persona

File persona revisions:

- Higher scalability: 512 TB total file capacity for 8 node 20000 system
- Network expansion: Separate static routes for each VLAN
- FPG alignment with 16k deduplication allocation units
- Quota accounting to exclude snapshot space
- Support for Windows 10 (Refer to the SPOCK website at <http://www.hpe.com/storage/spock> for the complete interoperability matrix.)

Known Issues with File Persona

Issue ID	Description
65361	SuSE SLES11 (first release) and SLES11 SP1 client does not support NFS4 ACL
73108	Creating a share with the name "0.0" shows as "0".
74742	In case a VFS or File Store is created containing special characters in its name, i.e. mt'ree0, and the file system is mounted in a passive node, it will not be possible to delete this VFS/File Store. The workaround for this is to mount the file system in the active node and then delete the VFS/File Store.
74914	Major alerts are generated when the user removes the non-existent snapshot. This alert needs to be ignored as this condition is valid and no user action is required.

Table Continued

Issue ID	Description
74941	When a SMB share creation operation is executed using a share name that is already in use for another SMB share, it won't be successfully created because this is a duplicated share. This action is improperly generating major alerts. When this alert is found, it's required to check the if this is a duplicate share, if so this alert can be ignored or the validity of the user operation can be checked.
73043	When AD is not responding during restore, the '+' sign is missing in the 'ls -l' output. Once the AD is available, name resolutions work fine resulting in POSIX ACL showing up for the POSIX clients and subsequently '+' sign would show up in the 'ls -l' output. This is just a display issue due to the unavailability of AD server. There is no data loss or data addition happening on-disk.
75420	When downgrading from 1.3 or 1.2 back to 1.3, 1.2, or 1.1, LDAP must be manually configured after downgrade.
75566	After cluster expansion, LDAP configuration does not automatically migrate to the new nodes. LDAP must be manually configured after expansion.
75936	There are registry key changes between 1.2 and 1.3, and while attempting to read the registry after upgrade to 3PAR 3.2.2 MU2, it has incorrect information in the registry and the certificate file can't be read from incorrect location. The workaround is to reconfigure the LDAP after upgrade.
76007	While accessing the SMB share, the message "The network path was not found" appears after the backup and restore operation of the config file at mtree level. The workaround to resolve this issue is to restart HP-SMB services.
74874	A thread blocks all actions in PML, resulting in a processing delay. If LDAP is not being used, remove LDAP from provider stacking order and restart the HP-SMB server.
75902	Changing bond mode causes loss of connectivity to all VLAN configured VFSIPs. VFSIPs for untagged networks do not seem to be adversely affected and shares remain accessible in either mode before and after changes. To recover, use <code>stopfs/startfs</code> on the nodes hosting the VFS.
75976	The user will not be able to perform NDMP Backup for certain Backup paths. While using Data Protector, user will observe following error: - BMA-NDMP: Bad catalog access for message #-1 in set 242. While using Netbackup, user will observe following error: - Error ndmpagent(pid=4424) ndmp_data_start_backup failed, status = 18 (NDMP_XDR_DECODE_ERR) There is no workaround available for the path where Backup fails, however, the user can mention other relevant directory paths and try Backup again. This issue is corrected in Unity 1.3 and later.
75627	After upgrading from 3.2.2 EGA to 3.2.2 MU2, if the customer runs <code>showalert</code> the output displays a major alert indicating a health issue. The customer can ignore this message. The LDAP component should work as expected.

3PAR OS 3.2.2 MU2 CLI Release Notes

Installation Notes for the CLI

Virus Checking

Virus checking is known to slow down and potentially cause issues with installation of the CLI. Before attempting an install or uninstall of the Remote CLI client, shut down all running applications and disable virus-checking software.

Deprecated Commands and Options

The deprecated options for the `cli`, `createuser`, and `setpassword` commands have been removed from the documentation.

Compatibility Changes in this Release

Remote CLI client versions earlier than Remote CLI client 3.2.2 cannot connect to the 3PAR OS, without using `-nosockssl` option.

Compatibility Changes in Next Release

The following options will be removed:

`cli: -pwf, -user, -password, and variable TPDPWFILE`

`createuser: -e`

`setpassword: -save, -saveonly, -file`

Installation Directory

Windows 32-bit: `C:\Program Files\Hewlett-Packard\HP 3PAR CLI`

Windows 64-bit: `C:\Program Files (x86)\Hewlett-Packard\HP 3PAR CLI`

UNIX and Linux: `/opt/hp_3par_cli`

Supported Operating Systems

For the list of supported operating systems, see the *HPE 3PAR CLI Remote Client* document on the SPOCK website at <http://www.hpe.com/storage/spock>.

Modifications to the CLI

Issue ID	Description
146781	Due to limited memory, the variable used in earlier releases to gather statistics for VVs has now been obsoleted by current code. The allocated memory was not freed up upon every call to <code>statvv</code> . This variable has been removed to stop the memory leak when <code>statvv</code> is run.
148636	Issue corrected with <code>cgcmd</code> when executing the <code>ddump</code> command.
151580	If a system is capable of supporting Flash Cache and it is enabled, CLI command <code>createflashcache</code> creates Flash Cache LDs per node with the node being owner of these LDs. Due to the issue in <code>checkhealth</code> , it thinks that connection to each of these LDs from other nodes is not an owner of Flash Cache LD. This issue is corrected in this release by avoiding such check that is done for other LDs which has multiple node ownership.

What's New in the CLI

The following new commands are added in 3PAR CLI 3.2.2 MU2:

Command	Description
<code>createfsroute</code>	Creates a route for a target address with a gateway
<code>removefsroute</code>	Removes an existing route for a target address
<code>setfsroute</code>	Modifies an existing route for a target address
<code>showfsroute</code>	Displays routes for target addresses

Known Issues in CLI

Command	Description
156023	3PAR CLI Linux client version 3.2.2.290 cannot connect to arrays running older 3PAR OS versions. This client gets the error "Badly formatted status response from server" when trying to connect to 3PAR arrays running older 3PAR OS versions such as 3.2.2 MU1, 3.2.2 GA, and 3.2.1 MUx. Please the Linux client from 3.2.2 MU1 (3.2.2.326) or 3.2.2 GA (3.2.2.290) instead. Those can connect to arrays running 3.2.2 MU2, as well as older releases. This issue does not exist with the 3PAR CLI client in other operating systems such as Windows, HP-UX, AIX and Solaris.

Changed commands

Command	Options added (unless stated otherwise)
createvfs	-snapquota
setfs	auth -clearcache
setfsquota -clear	-uid, -gid
showfs -smb	Output changed
showfsndmp	Changed output format

3PAR OS 3.2.2 MU2 CIM API Release Notes

Modifications to the CIM API Software

Issue ID	Description
145564	TPD_HostedStoragePool association returns all CIM_StoragePools associated with the StorageSystem even when client requested only TPD_StoragePool in ResultClass. This has been corrected.
146214	New event is added when CIM configuration is changed via setcim CLI command.
151226	The TPD_StorageConfigurationService::ModifySynchronization(detach) operation would sometimes expire when the volume being detached was "busy" being referenced by an internal maintenance job on the 3PAR system. This issue has been corrected.
152210	A new cimserver policy has been added to set the SMI-S Interop namespace such that it conforms to the SMI-S 1.6 specification. Use the setcim CLI command to set the no_use_pegasus_interop_namespace policy for SMI-S Interop namespace compliance. The default policy is use_pegasus_interop_namespace, which is backward compatible with previous releases for cimserver.
153854	The method TPD_StorageConfigurationService::CreateReplica occasionally reports that it was unable to create a snapshot volume when in fact it did create the volume. The problem occurred because of an internal caching error, which has now been corrected.

What's New with the CIM API Software

A new cimserver policy has been added to set the SMI-S Interop namespace such that it conforms to the SMI-S 1.6 specification. Use the setcim CLI command to set the no_use_pegasus_interop_namespace policy for SMI-S Interop namespace compliance. The default policy is use_pegasus_interop_namespace, which is backward compatible with previous releases for cimserver.

NOTE:

Support for TLS v1.0 and v1.1 will be deprecated and removed in a future release, making TLS v1.2 the only supported version. Please migrate your client to use TLS v1.2 and the ciphers DHE-RSA-AES256-GCM-SHA384 and/or DHE-RSA-AES128-GCM-SHA256 as soon as possible.

3PAR OS 3.2.2 MU2 Web Services API Release Notes

Modifications to the Web Services API Software

Issue ID	Description
144090	WSAPI URL is added to showwsapi output.
144650	Issues corrected when a hostset comment contains certain characters such as " or [.
146174	New event is added when WSAPI configuration is changed. In the following condition, this new event will occur: <ul style="list-style-type: none">• WSAPI server is started (startwsapi)• WSAPI server is stopped (stopwsapi)• WSAPI configuration is changed (setwsapi)
150067	Issues corrected with PUT of /qos on vvset.
152206	There were limited memory resources in WSAPI server when establishing sessions. This has been corrected.

What's New with the Web Services API Software

- Added the following support for remotecopytargets object:
 - GET
 - PUT of target policy (mirrorConfig)
- New latencyGoaluSecs in qos object. Use this to set QoS latencyGoal in usec.
- New differentSecondaryWWN option when admitting a volume to a remotecopygroup. When used with volumeAutoCreation set to TRUE, this ensures a different WWN is used on the secondary volume. Without this option and with volumeAutoCreation set to TRUE, the same WWN will be used for both primary and secondary volumes.
- Web services API now supports TLS v1.1 and v1.2 as well as two new ciphers, DHE-RSA-AES256-GCM-SHA384 and DHE-RSA-AES128-GCM-SHA256.

NOTE:

Support for TLS v1.0 and v1.1 will be deprecated and removed in a future release, making TLS v1.2 the only supported version. Please migrate your client to use TLS v1.2 and the above two new ciphers as soon as possible.

Known Issues

Issue ID	Description
106458	Certain values are not included in response from GET /cpgs if they are default values.

3PAR OS 3.2.2 EMU2 Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 EMU2 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.

CAUTION:

- 3PAR 3.2.2 EGA Patch 35 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.
- 3PAR 3.2.2 MU1 Patch 37 must be installed prior to upgrading from 3PAR 3.2.2 MU1 to a later version.

Supported Platforms

For details of supported HPE 3PAR StoreServ Storage, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

More information

<http://www.hpe.com/storage/spock>

Components

Component	Version
OS	3.2.2.390
CLI Client	3.2.2.390
SNMP Agent	1.8.0
File Persona	1.2.1.3-20160211
Drive Cage Firmware:	
DC4 Firmware	2.64
MCU Firmware (OKI)	4.8.28
MCU Firmware (STM)	5.2.52
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	4044
DCS5 / DCS 6 Firmware	1.90

Table Continued

Component	Version
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.06
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x02
Emulex LPe12004 HBA Firmware	02.03.x02
Emulex LPe16002 HBA Firmware	10.6.296.0
Emulex LPe16004 HBA Firmware	10.4.395.0
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

Modifications to the OS

3PAR OS 3.2.2 EMU2 combines all of the modifications and features provided by 3PAR OS 3.2.2 MU2 Patch 11, Patch 14, and Patch 15. Refer to the release notes documents for each patch for a full list of modifications, features and supported drives. To obtain copies of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.

3PAR OS 3.2.2 EMU2 also includes the following modifications:

- Addresses an issue during cleanup/removal of Adaptive Flash Cache (AFC) that would lead to an unexpected system restart.
- Prevents an unexpected array restart when using
updatevv
with snapshots present.
- Provides enhanced monitoring of Remote Copy Fibre Channel ports to reduce the frequency of false positive link down messages.
- Corrects an issue where a new VV could not be added to an exported VVset.

- Corrects an issue in which an unexported virtual volume deletion may have occurred when finishing an upgrade to HPE 3PAR OS 3.2.2 from pre-HPE 3PAR OS 3.2.2.
- Addresses an online upgrade issue with remote copy enabled which causes an unexpected shutdown.

3PAR OS 3.2.2 MU3 Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 MU3 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to the **Hewlett Packard Enterprise Support Center** <http://www.hpe.com/info/enterprise/docs>.

Warnings, Cautions and Notes

CAUTION:

- 3PAR 3.2.2 EGA Patch 43 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.
- 3PAR 3.2.2 MU1 Patch 37 must be installed prior to upgrading from 3PAR 3.2.2 MU1 to a later version.

NOTE:

Contact your Hewlett Packard Enterprise account representative to review the requirements for enabling the 3PAR Remote Copy Asynchronous Streaming feature.

Supported Platforms

For details of supported HPE 3PAR StoreServ Storage, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

More information

<http://www.hpe.com/storage/spock>

Components Included in this Release

Component	Version
CLI Server	3.2.2.530
CLI Client	3.2.2.530
SNMP Agent	1.8.0
File Persona	1.2.2.5-20160603
Drive Cage Firmware:	

Table Continued

Component	Version
MCU Firmware (OKI)	4.8.28
MCU Firmware (STM)	5.2.52
DC1 Firmware	4.44
DC2 / DC4 Firmware	2.64
DC3	08
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	406a
DCS5 / DCS6 Firmware	1.93
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.07
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x02
Emulex LPe12004 HBA Firmware	02.03.x02
Emulex LPe16002 HBA Firmware	10.6.248.3
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

HDD/SDD Firmware Included in this Release

Type	Capacity	3PAR Drive Model	Speed	3PAR StoreServ Model Supported				Firmware
				7000	10000	8000	20000	
HDD	8 TB	SMKP8000S5xeN7.2	7.2K	No	No	Yes	Yes	3P00
HDD	2 TB	SMKR2000S5xeF7.2	7.2K	No	No	Yes	Yes	3P03
SSD	400 GB	AREX0400S5xnNTRI	150K	No	Yes	No	No	3P01
HDD	2 TB	SMKR2000S5xeF7.2	7.2K	Yes	No	No	No	3P03
HDD	4 TB	HAKP4000S5xeN7.2	7.2K	Yes	No	Yes	Yes	3P02
HDD	6 TB	HAKP6000S5xeN7.2	7.2K	Yes	No	Yes	Yes	3P02
SSD	400 GB	AREX0400S5xnNTRI	150K	Yes	No	Yes	Yes	3P01
HDD	4 TB	SMKR4000S5xeF7.2	7.2K	No	No	Yes	Yes	3P03
HDD	6 TB	SMKR6000S5xeF7.2	7.2K	Yes	Yes	Yes	Yes	3P03
HDD	2 TB	SMKR2000S5xeN7.2	7.2K	Yes	Yes	Yes	Yes	3P02
HDD	4 TB	SMKR4000S5xeN7.2	7.2K	Yes	Yes	Yes	Yes	3P02
HDD	6 TB	SMKR6000S5xeN7.2	7.2K	Yes	Yes	Yes	Yes	3P02
HDD	1.2 TB	HCBF1200S5xeF010	10K	Yes	No	Yes	Yes	3P03
HDD	600 GB	HCBF0600S5xeN010	10K	No	Yes	Yes	Yes	3P03
HDD	1.2 TB	HCBF1200S5xeN010	10K	Yes	Yes	Yes	Yes	3P03
HDD	1.8 TB	HCBF1800S5xeN010	10K	Yes	Yes	Yes	Yes	3P03
HDD	600 GB	HKCF0600S5xeF015	15K	Yes	Yes	Yes	Yes	3P03
HDD	300 GB	HKCF0300S5xeN015	15K	Yes	Yes	No	No	3P03
HDD	600 GB	HKCF0600S5xeN015	15K	Yes	Yes	No	No	3P03
HDD	8 TB	SMKP8000S5xeF7.2	7.2K	No	No	Yes	Yes	3P00
SSD	7.68 TB	AREA7680S5xnNTRI	SSD	Yes	No	Yes	Yes	3P00
HDD	1 TB	SAVN1000S5xeN7.2	7.2K	No	No	No	No	3P04
HDD	2 TB	SAVN2000S5xeN7.2	7.2K	Yes	No	No	No	3P04

Table Continued

Type	Capacity	3PAR Drive Model	Speed	3PAR StoreServ Model Supported				Firmware
				7000	10000	8000	20000	
HDD	2 TB	SMEG2000S5xnN7.2	7.2K	Yes	Yes	No	No	3P02
HDD	4 TB	SMEG4000S5xnN7.2	7.2K	Yes	Yes	No	No	3P02
HDD	2 TB	SMEG2000S5xnF7.2	7.2K	Yes	Yes	No	No	3P01
SSD	3.84 TB	DOPM3840S5xnNMRI	SSD	Yes	No	Yes	Yes	3P04
HDD	600 GB	STHB0600S5xeN010	10K	Yes	No	Yes	Yes	3P02
HDD	1.2 TB	STHB1200S5xeN010	10K	Yes	No	Yes	Yes	3P02
HDD	1.8 TB	STHB1800S5xeN010	10K	Yes	No	Yes	Yes	3P02
SSD	480 GB	DOPE0480S5xnNMRI	100K	Yes	No	Yes	Yes	3P07
SSD	480 GB	DOPE0480S5xnNMRI	100K	Yes	No	Yes	Yes	3P07
SSD	1920 GB	DOPE1920S5xnNMRI	100K	Yes	No	Yes	Yes	3P07

What's New in the OS

3PAR OS 3.2.2 MU3 provides all the benefits provided by 3PAR OS 3.2.2 EMU2 and includes several revisions.

Direct attach copper (DAC) cable support is expanded for HPE 3PAR StoreServ systems. Passive DAC connectivity is now available for 3PAR StoreServ 8000 and 20000 platforms. There is no change with existing DAC connectivity support for 3PAR StoreServ 7000 and 10000 platforms; however, not all DAC cables supported on the 3PAR 7000 and 10000 platforms are supported in the 3PAR OS 3.2.2 MU3 release.

DAC cable support for 3PAR StoreServ 8000 and 20000 platforms requires 3PAR OS 3.2.2 MU3. File* protocol is only supported by 3PAR OS 3.2.2 MU3. 3PAR DAC supported configurations with 3.2.2 MU3 require a LAN switch between the 3PAR (target) and host initiator (Adapter). Direct connect between the 3PAR (target) and host initiator (Adapter) without a switch is not supported, even if a DAC cable is used.

NOTE:

The term “direct” refers to the direct attach of the cable to the SFP+ housing, instead of attaching to a SFP+ module that plugs into the SFP+ housing.

The table below lists the DAC cables supported with 3PAR OS 3.2.2 MU3. All protocols across all cables listed in this table are supported by 3PAR OS 3.2.2 MU3.

Table 1: DAC Support in 3PAR OS 3.2.2 MU3

	3PAR StoreServ Platforms and Required DAC OS Support				
DAC Description	7000	10000	8000	20000	Speed/Protocols Supported
HPE X240 10G SFP+ to SFP+ 0.65m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	Not supported	Not supported	10GbE, iSCSI, FCoE, File*, RCIP
HPE X240 10G SFP+ to SFP+ 1.2m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE X240 10G SFP+ to SFP+ 3m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE X240 10G SFP+ to SFP+ 5m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE x240 QSFP+ 4x10G SFP+ 1m DAC Cable	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE X240 10G SFP+ to SFP+ 7m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	Not supported	Not supported	10GbE, iSCSI, FCoE, File*, RCIP
HPE x240 QSFP+ 4x10G SFP+ 3m DAC Cable	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE x240 QSFP+ 4x10G SFP+ 5m DAC Cable	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE X242 10G SFP+ to SFP+ 1m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE X242 10G SFP+ to SFP+ 3m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE X242 10G SFP+ to SFP+ 7m DAC Cable	3PAR OS 3.1.3 or later	3PAR OS 3.1.3 or later	Not supported	Not supported	10GbE, iSCSI, FCoE, File*, RCIP
HPE C-series 3m Passive Copper SFP+ Cable	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP
HPE C-series 5m Passive Copper SFP+ Cable	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	3PAR OS 3.2.2 MU3	10GbE, iSCSI, FCoE, File*, RCIP

PersonaProfile

Starting with 3PAR OS 3.2.2 MU3, there is a new system parameter in the 3PAR OS called PersonaProfile, which allows a 3PAR system to be in one of the following two profiles:

- **block-only:** For example, File Persona cannot be configured and no memory is reserved for File Persona.
- **block-preferred:** For example, File Persona can be configured and memory is reserved for File Persona.

PersonaProfile settings are decided based on certain rules depending on the configuration of the array. These rules are applicable to all 7000c, 8000 and 20000 series arrays and can be subdivided as install time rules and upgrade time rules.

The install time rules which take effect for new arrays shipped with 3PAR OS 3.2.2 MU3 include:

- PersonaProfile is set to **block-preferred** if the array is of type 20800, or the array has empty PCI slots and is of type 7200c/7400c/8200/8400 and does not have any TDVVs, or the array has one of the following add-on Ethernet cards installed:
 - 3PAR StoreServ 7000c 2-port 10Gbps Ethernet Adapter E7X96A
 - 3PAR StoreServ 7000c 4-port 1Gbps Ethernet Adapter E7X97A
 - 3PAR StoreServ 8000 4-port 1Gbps Ethernet Adapter - H6Z05A
 - 3PAR StoreServ 8000 2-port 10Gbps Ethernet Adapter - E7Y70A
 - 3PAR StoreServ 20000 2-port 10Gbps Ethernet Adapter for File Persona - C8S95A
 - 3PAR StoreServ 20000 2-port 10Gbps Upgrade Ethernet Adapter for File Persona - C8S99A

For everything else, PersonaProfile is set to **block-only**.

These upgrade time rules take effect when arrays are upgraded to 3PAR OS 3.2.2 MU3:

- PersonaProfile is set to **block-preferred** if the array has File Persona license present, if the array is of type 20800, or the array has empty PCI slots and is of type 7200c/7400c/8200/8400, or the array has one of the following add-on Ethernet cards installed:
 - 3PAR StoreServ 7000c 2-port 10Gbps Ethernet Adapter E7X96A
 - 3PAR StoreServ 7000c 4-port 1Gbps Ethernet Adapter E7X97A
 - 3PAR StoreServ 8000 4-port 1Gbps Ethernet Adapter - H6Z05A
 - 3PAR StoreServ 8000 2-port 10Gbps Ethernet Adapter - E7Y70A
 - 3PAR StoreServ 20000 2-port 10Gbps Ethernet Adapter for File Persona - C8S95A
 - 3PAR StoreServ 20000 2-port 10Gbps Upgrade Ethernet Adapter for File Persona - C8S99A

For everything else, PersonaProfile is set to **block-only**.

The storage administrator should contact Hewlett Packard Enterprise support to change the PersonaProfile settings.

Modifications to the OS

3PAR OS 3.2.2 MU3 combines all of the modifications and features provided by 3PAR OS 3.2.2 EMU2 and includes the following modifications:

Issue ID	Description
115477	Addresses an issue in which the array can become unresponsive in the context of a registered state change notification (RSCN) storm, where the name server in the switch sends many back-to-back notifications of topology changes in very rapid succession.
117865	Addresses a concurrency issue between virtual volume (VV) unmap request and VV operations like VV close, VV delete, etc.
118170	Resolves issues where a controller node unexpectedly restarts if the <code>controlport</code> CLI commands are issued in a particular sequence on systems configured with RC.
123096	Corrects an in issue with displaying the power-supply inventory information in the DCS7 drive enclosures.
126873	A warning message is now printed during servicemag start if the magazine bypass is not successful, but the servicemag now proceeds.
128379	Resolves an issue with certain power cooling modules (PCM) where transition from building power to UPS power causes a brief loss of access to physical disk (PD) drives.
129554	Prevents unexpected controller node restart during an offline upgrade.
133562	Prevents stalls during iSCSI host I/O to array.
137184	Addresses a memory allocation issue that caused an unexpected controller node restart by reducing the memory allocation size.
138981, 156705, 159768	Addresses an issue in which constrained memory resources in 128-byte structure results in controller node restart.
140546	The lifetime counts of uncorrectable errors on PDs are now monitored. When it exceeds preset limits, an event is generated and the drive is evacuated so it can be replaced.
142444	Resolves an issue in which some edge condition locks were not invoked, leading to unexpected controller node restarts.
142494	Corrects an issue encountered when using the <code>removevln</code> command on a renamed virtual volume with dry run flag <code>removevln -dr</code> and/or pattern flag <code>removevln -pat</code> returns “export not found” and/or “No matching vluns” alerts.
145460	Prevents unexpected data integrity field (DIF) alerts reported against controller nodes in the array. These alerts will now only be returned if a true issue exists.
145970	Corrects an issue in which the resync snapshot given in <code>startcopy group</code> command was removed while it was syncing.

Table Continued

Issue ID	Description
146740	The SP now collects <code>showeventlog</code> info if the array has a time zone with GMT followed by numbers (for example: GMT+5, GMT-5).
148734	Corrects an issue in which unexpected PCM state transitions from failed to normal.
149655	Resolves an issue in which, when the same initiator logs in again with a different device ID, two entries for the same initiator are created in 8 Gb Fibre Channel (FC) drivers.
150427	Prevents an unexpected array restart when a log requires additional CPU time.
150821	Unsuccessful attempts to read network routes no longer result in an unexpected restart of the netc process.
151256	Corrects an issue in which a host sends a Report Timeout Values (RTV) command to the storage array and unexpected values are returned, resulting in I/O timeout.
151791	Addresses an unexpected controller node restart while duplicating LD memory pages to the backup controller node.
152388	Resolves issues with the sequencer initialization for remote copy that cause issues during upgrades or controller node reboots.
152506	Improves the reliability with which non-network master controller nodes sync to the network master controller node's NTP time.
152636	Improves algorithm for preserved volume data and adds sufficient checking to ensure that all data to be saved is valid and saved.
152691	Addresses an issue with memory inconsistencies in the SAS driver space.
152728	Prevents system manager stalls while installing 3PAR OS patches.
152884	Prevents the DCS5/DCS6 drive enclosures (cages) from encountering an internal I2C communication issue that cause the drives in bays 3, 8, 9, 13, 14, 18, 19 to go offline.
153066	The <code>controlport login</code> command is now implemented for model numbers LPe16002 (two-port) and LPe16004 (four-port) 16 Gb Fibre Channel (FC) host bus adapters (HBAs). This command is only used internally by the HPE Online Import Utility (OIU).
153150	A calculation issue which caused repeated unexpected restarts of the system manager is addressed when calculating the LD block to free.
153400	Corrects an issue the causes an unexpected alert stating the links are down on all Remote Copy over Fibre Channel (RCFC) ports.
153560	Prevents unexpected controller node restart when a PD is dismissed directly following an LD deletion.
153872	Improves memory resource usage in the VASA Provider.

Table Continued

Issue ID	Description
154208	Prevents unexpected alerts during a port reset if the Internet Storage Name Service (iSNS) is configured on a tagged VLAN and the VLAN is removed.
154333	Extends the retention time of hires SR data by increasing the growth limit to 400 GB.
154453	Addresses an issue in which controller nodes unexpectedly restart when unnecessarily validating DIF.
154469	Corrects an unexpected controller node restart issue after unexpected system manager restart during volume conversions.
154739	Resolves an issue in which incorrect use of array index during I/O abort processing in the SAS HBA driver causes unintended resets of the disk port.
155358	Prevents loss of host connectivity due to command timeouts caused by exhaustion of array port resources.
155558	Servicemag now prevents LD allocation and chunklet movement on the serviced physical disks.
155624	Improves memory resource utilization for the D3650 and D3750 (DCS5/DCS6) drive enclosures.
156061	cimserver is now able to generate enumerate instances for a number of classes if the array has an all-numeric name.
156299	Corrects an issue in which the <code>ModifyReplicaSynchrononization</code> resync operation stalls for periodic remote copy groups represented in SMI-S as Asynchronous TPD_RemoteReplicaionGroup instances.
156309	Provides SSMC with a new event type under <code>COMP_SW_RMM_TARGET sw_rmm_target</code> . This event will be generated every time Quorum Witness (QW) is auto activated. The substring associated with this event is "Associated QW has started."
156562	Corrects a controller node stall in deduplication read I/O path.
156563	Corrects an issue in which after setting the management port to 100/FULL, shownet still displays AutoNeg=YES instead of AutoNeg=NO.
156987	Resolves an issue in which when creating or removing a sub-LUN (logical unit number), an unrelated virtual LUN (VLUN) would incorrectly disconnect.
157006	Corrects an issue in which an unexported virtual volume deletion may have occurred when finishing an upgrade to 3PAR OS 3.2.2 from pre-3PAR OS 3.2.2.
157635	Resolves an issue in which, if a single node is intentionally restarted while the array is in a blocked state awaiting I/O from a faulty remote copy system, then an unexpected multinode restart may occur when the remote system resumes normal operation.

Table Continued

Issue ID	Description
157811, 154453	Addresses a defragmentation issue in the deduplication I/O path.
157950	ATS commands sent by VMware hosts no longer unexpectedly abort due to timeout.
158245	The SMI-S TPD_StorageVolume object now includes the property UsedUserDataBlocks which corresponds to the value displayed in the "Used Usr Space" column with the CLI command <code>showvv -space</code> .
158669	Corrects an issue in which an unexpected flag indicating that VLUN templates should not be translated into any new active VLUNs could be re-enabled if it is set on a controller node at the time the controller node is restarted and that controller node becomes the new master node.
159183	Resolves an issue in which adaptive optimization (AO) does not complete the move of VV regions at offsets beyond 2 TB.
159288, 169517	Improves Deduplication Store (DDS) defragmentation speed.
159350	Addresses an issue during cleanup/removal of Adaptive Flash Cache (AFC) that would lead to an unexpected system restart.
159542, 164010	Corrects an issue with VVset growth when multiple hosts are present in the VVset. LUN allocation within a VVset requires the LUN IDs to be sequential. VVset growth will not complete if a duplicate LUN ID is already occupied.
159600	Provides enhanced monitoring of Remote Copy Fibre Channel ports to reduce the frequency of false positive link down messages.
159782	Stops an RC group if it is taking longer than 45 seconds to replicate an I/O in Sync Mode RC groups.
159823	Prevents unnecessary SAS port resets.
160233	Corrects an issue in which chunklet initialization (CHINIT) will not proceed on a physical disk (PD) under servicemag.
160352, 157432	Corrects miscabling cases that result in unusable ports which require a reboot of the impacted controller nodes after the miscabling condition is resolved.
160438, 166342	Prevents unexpected array restarts due to a held DDC lock.
160672, 162165, 162181, 162184, 162185	Various open source packages, such as libc, have been updated to address security vulnerabilities.

Table Continued

Issue ID	Description
160808	Prevents iSCSI host connectivity stalls when multiple ports go offline or online at the same time.
161161	Resolves an issue in which incorrect use of array index during I/O abort processing in the SAS HBA driver causes unintended resets of the disk port.
161458	WSAPI now services more than one active concurrent session for arrays with six controller nodes, or any odd number of controller nodes, and no longer displays "Service Too Busy" message.
161581	Addresses controller node restart when region move on the currently active LD can split the remote write into two writes spanning two LDs both owned by same controller node.
161738	Corrects an issue in which an unexpected alert is posted when free memory is low due to high page cache usage.
161945	Adds improvement that aborts Extended Copy SCSI commands if the target volumes on the 3PAR array are exported to I/O paths that are not ALUA active.
162152	Corrects a direct connect issue which prevented 16 Gb FC HBAs from connecting to host ports.
162538	Currently, CLI honors the actual value set in the system parameter (SessionTimeout). Now tpdctl will also time out SSMC/MC/CLX, etc. connections based on the system parameter, with the exception that tpdctl will time out idle sessions after one hour if the system parameter is set lower than one hour. In a future release, the minimum will be enhanced to honor a time out value as low as three minutes.
162575	Resolves an issue in which the deduplication space-saving estimation tool was creating large log files.
162639	Provides a configurable parameter to modify the byte-per-sector field in SCSI mode page 3 to maintain backward compatibility.
162821	Prevents controller node restarts when changing a port from a mode that uses NPIV (persistent ports or peer motion) to a mode that does not.
162897	Resolves an issue which causes the <code>Cache Degraded</code> alert to be generated prematurely.
163018	Addresses an issue in which some VMware versions may send unsupported commands to the PE LUN (LUN 256). Such commands are currently returned with sense data 0x5 0x25 0x0. This response causes VMware to encounter an unexpected PDL alert on the LUN. The response is now changed to 0x5 0x20 0x0 to avoid this issue.
163295	Deduplication <code>showvv -s</code> enhancement improves user experience in terms of used TDVV/DDS size.

Table Continued

Issue ID	Description
165022	Prevents a memory allocation issue that results in an unexpected controller node restart due to a buildup of stale Secure Shell (SSH) sessions. Please note the following: <ul style="list-style-type: none"> The number of SSH sessions and CLI over SSH sessions are not the same; the CLI will still reject CLI sessions when the CLI reaches its threshold. The SSH connection is rejected when an ICMP reject is encountered. Remote CLI, CLX, SSMC, and other products are not affected by this change.
165282	Corrects a cluster stall for a detected token inconsistency on rebooting controller nodes.
165524	Prevents VV resizing when the system manager is restarted if the VV is not aligned on 256 MB boundaries.
165806	Corrects an issue which prevented the slow disk checker from identifying certain slow SSD disks and removing the slow disks from the system. This can lead to degraded system performance.
165992	The D3650 and D3750 (DCS5/DCS6) drive enclosure firmware now properly sets the display code as instructed by the storage controller.
166342	Provides recovery to allow an upgrade to continue without intervention when a controller node restart occurs during an online upgrade.
167059	Corrects an issue in which POST/credentials request with null or empty username or password can lead to WSAPI server restart.
167128	Resolves an issue in which during 3PAR OS upgrade, after first controller node reboot, the system manager becomes unresponsive to CLI commands.
167219	<code>ddcscan</code> now uses one bitmap for DDS and Deduplication Client (DDC) to improve memory resources.
167309	Addresses an issue that occurs when a remote read is requested to a controller node when “node down recovery” is in progress. The controller node that is performing “node down recovery” no longer restarts due to an unexpected lock step timeout.
168271	Corrects issues with <code>statqos -rw</code> .
168917	Corrects an issue that causes a controller node restart when DIF is enabled.
169886	Vulnerable cluster memory pages are now reserved and excluded from use by software or HBA write operations.
169984	Mitigates repetitive unexpected array restarts by enhancing <code>checkvv</code> for TDVVs.
178185	Addresses an issue in which memory resources are constrained when cage SFP information is read.

Known Issues with the OS

Issue ID	Description
159212	After removing the last TDVV in a common provisioning group (CPG), DDS stalls and the DDS volume is not removed.
160232	If volumes imported using the Online Import Utility (OIU) tool have TPGID between 3 and 256, they cannot be added to RC groups with PP configured. The workaround is to change the TPGID of the volume to 1 using <code>setvv -settpgid <tpgid> <vvname></code> .

3PAR OS Patches Included in this Release

This list includes all 3PAR OS 3.2.2 MU2 patches included in this release since the last base maintenance update. To obtain copies of the patch release notes documents, go to <http://www.hpe.com/info/enterprise/docs>.

- 3PAR OS 3.2.2 MU2 Patch 11
- 3PAR OS 3.2.2 MU2 Patch 14
- 3PAR OS 3.2.2 MU2 Patch 15
- 3PAR OS 3.2.2 MU2 Patch 18
- 3PAR OS 3.2.2 MU2 Patch 19
- 3PAR OS 3.2.2 MU2 Patch 20
- 3PAR OS 3.2.2 MU2 Patch 22
- 3PAR OS 3.2.2 MU2 Patch 23
- 3PAR OS 3.2.2 MU2 Patch 24
- 3PAR OS 3.2.2 MU2 Patch 26
- 3PAR OS 3.2.2 MU2 Patch 27
- 3PAR OS 3.2.2 MU2 Patch 28
- 3PAR OS 3.2.2 MU2 Patch 29
- 3PAR OS 3.2.2 MU2 Patch 30
- 3PAR OS 3.2.2 MU2 Patch 33

Modifications to File Persona

The version of File Persona software included with 3PAR OS 3.2.2 MU3 addresses a number of customer-found and CentOS security issues to improve the overall product quality:

Issue ID	Description
75244	Resolves an issue in which, while Lightweight Directory Access Protocol (LDAP) server is down or LDAP service is stopped, LDAP health and SSH controller nodes stall. This is corrected and SSH to controller nodes is now successful.
75389	Corrects "base of search" configuration in LDAP if user tries to map a share/or accessing already mapped share using AD or local user. The authentication is now successful.
75905	Resolves issue in which use of <code>setfs bond <N></code> to change the File Persona bonding mode caused connectivity stalls to VLAN-tagged addresses until the File Persona services were restarted.
76264	LDAP now remains configured during product upgrade.
76394	Password expiration policy for local users has changed to "never expires". In previous releases the default required passwords to be changed for local users after 30 days. Customers upgrading to this release will have to change any local passwords before the "never expires" policy takes effect.
76429	Addresses an issue that resulted in slowly increasing memory usage over time such that after a year or more of up time some impact to performance might occur.
77066	Corrects memory allocation issues and now the user can perform NetBackup/Data Protector (NDMP) backup for all backup paths.
77423	Addresses an issue during deactivation of an FPG, a timeout in the deactivation could result in the VFS IP addresses remaining active on the node after deactivation. This prevents activation of the IP addresses on a new node in a failover scenario and resulted in a data unavailability for clients. If such a scenario were now to occur, the IP addresses will be properly deactivated on the original node such that a failover will succeed without resulting in an unavailability for clients.
80590	If a failure occurs when trying to delete a file store, it is now left in a state where snapshots can be taken. Previously when this occurred, the file store would be left in a state where snapshots could not be taken and an alert would indicate, "Deletion did not complete because File store xyz is not empty. Please clean up user files and repeat the operation. This File Store is no longer to be used for snapshots." Now the message indicates, "Deletion did not complete because File store xyz is not empty. Please clean up user files and repeat the operation." The file store is left in a state where snapshots will work.
83161	Resolves an issue where SMB shares would become temporarily unavailable.
155198	Corrects an issue in which when File Persona is started by a LDAP user, the operation restarts and leaves File Persona ports uncleaned, which causes the subsequent <code>startfs</code> to restart.

Known Issues with File Persona

Issue ID	Description
83978	Snapshot reclamation only runs in DEFAULT (MAXSPACE) mode. This is because the plugin is not properly enabling the strategy setting when starting the task. This causes the task to default to the DEFAULT strategy which is MAXSPACE. Therefore, the task always runs with the MAXSPACE strategy even if the MAXSPEED is requested. There is no error message.

What's New in the CLI

The following improvements are added in 3PAR CLI 3.2.2 MU3:

- Adds support for x86 Solaris CLI client.
- The location of Solaris SPARC installer has changed from
`/cdrom/cli/solaris/setup.bin`
to
`/cdrom/cli/solaris-sparc/setup.bin`.

Modifications to the CLI

Issue ID	Description
141531	Suitable warning message is added for <code>servicemag -log</code> option.
147052, 153581	Resolves an issue in which the controller node rebalance command <code>tunenodech</code> results in an "Unknown LD creation pattern" alert.
148623	Updated additional warnings of running <code>setsysmgr wipe</code> and <code>-f</code> option.
156023	Resolves an issues that result in an unexpected "Badly formatted status response from server" alert when trying to connect to 3PAR arrays running older 3PAR OS versions, such as 3PAR OS 3.2.2 MU1 and 3.2.2 GA. Please use the Linux client from 3PAR OS 3.2.2 MU1 (3.2.2.326) or 3.2.2 GA (3.2.2.290) instead. Those can connect to arrays running 3PAR OS 3.2.2 MU2, as well as older releases.
162538	<code>tpdtcl</code> now honors the system parameter <code>SessionTimeout</code> and will timeout idle sessions.
162804	Resolves an issue in which using multiple remote CLI sessions concurrently causes unexpected stall when exiting.
168819	Corrects an issue that was encountered when CLI <code>showvv</code> commands were issued during <code>updatevv</code> and caused the cache server to encounter an incomplete VV tree.

3PAR OS 3.2.2 MU4 Release Notes

OS Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 MU4 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*.

All the content from previous 3.2.2 maintenance updates are included in 3PAR OS 3.2.2 MU4. For a list of patches included in this maintenance update, please see **3PAR OS Patches Included in this Release**.

More information

<http://www.hpe.com/info/storage/docs/>

<http://www.hpe.com/support/hpesc>

Warnings, Cautions and Notes

CAUTION:

- 3PAR 3.2.2 EGA Patch 43 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.
- 3PAR 3.2.2 MU1 Patch 37 must be installed prior to upgrading from 3PAR 3.2.2 MU1 to a later version.

NOTE:

Contact your Hewlett Packard Enterprise account representative to review the requirements for enabling the 3PAR Remote Copy Asynchronous Streaming feature.

Supported Platforms

For details of supported HPE 3PAR StoreServ Storage, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

More information

<http://www.hpe.com/storage/spock>

Components Included in 3PAR OS 3.2.2 MU4

Component	Version
CLI Server	3.2.2.612 (MU4)
CLI Client	3.2.2.612
System Manager	3.2.2.612 (MU4)

Table Continued

Component	Version
Kernel	3.2.2.612 (MU4)
SNMP Agent	1.8.0
File Persona	1.2.2.6-20161017
Drive Cage Firmware:	
MCU Firmware (OKI)	4.8.29
MCU Firmware (STM)	5.2.53
DC1 Firmware	4.44
DC2 / DC4 Firmware	2.64
DC3	08
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	4078
DCS5 / DCS6 Firmware	1.93
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.08
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x11
Emulex LPe12004 HBA Firmware	02.03.x11
Emulex LPe16002 HBA Firmware	10.6.248.4
Emulex LPe16004 HBA Firmware	10.6.248.4
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00

Table Continued

Component	Version
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

What's New in the OS

3PAR OS 3.2.2 MU4 provides all the benefits provided by 3PAR OS 3.2.2 MU3 and includes several revisions.

Starting with 3PAR OS 3.2.2 MU3, there is a new system parameter in the 3PAR OS called PersonaProfile, which allows a 3PAR system to be in one of the following two profiles:

- **block-only:** For example, File Persona cannot be configured and no memory is reserved for File Persona.
- **block-preferred:** For example, File Persona can be configured and memory is reserved for File Persona.

PersonaProfile settings are decided based on certain rules depending on the configuration of the array. These rules are applicable to all 7000c, 8000, and 20000 series arrays and can be subdivided as install time rules and upgrade time rules. In 3PAR OS 3.2.2 MU4, these rules have been changed.

The install time rules which take effect for new arrays shipped with 3PAR OS 3.2.2 MU4 include:

- PersonaProfile is set to **block-preferred** if the array has one of the following add-on Ethernet cards installed:
 - 3PAR StoreServ 7000c 2-port 10Gbps Ethernet Adapter E7X96A
 - 3PAR StoreServ 7000c 4-port 1Gbps Ethernet Adapter E7X97A
 - 3PAR StoreServ 8000 4-port 1Gbps Ethernet Adapter - H6Z05A
 - 3PAR StoreServ 8000 2-port 10Gbps Ethernet Adapter - E7Y70A
 - 3PAR StoreServ 20000 2-port 10Gbps Ethernet Adapter for File Persona - C8S95A
 - 3PAR StoreServ 20000 2-port 10Gbps Upgrade Ethernet Adapter for File Persona - C8S99A

For everything else, PersonaProfile is set to **block-only**.

These upgrade time rules take effect when arrays are upgraded to 3PAR OS 3.2.2 MU4:

- PersonaProfile is set to **block-preferred** if File Persona is already configured on the array, or if the array has one of the following add-on Ethernet cards installed:
 - 3PAR StoreServ 7000c 2-port 10Gbps Ethernet Adapter E7X96A
 - 3PAR StoreServ 7000c 4-port 1Gbps Ethernet Adapter E7X97A
 - 3PAR StoreServ 8000 4-port 1Gbps Ethernet Adapter - H6Z05A
 - 3PAR StoreServ 8000 2-port 10Gbps Ethernet Adapter - E7Y70A

- 3PAR StoreServ 20000 2-port 10Gbps Ethernet Adapter for File Persona - C8S95A
- 3PAR StoreServ 20000 2-port 10Gbps Upgrade Ethernet Adapter for File Persona - C8S99A

For everything else, PersonaProfile is set to **block-only**.

The storage administrator should contact Hewlett Packard Enterprise support to change the PersonaProfile settings.

More information

<http://www.hpe.com/support/hpesc>

Modifications to the OS

3PAR OS 3.2.2 MU4 combines all of the modifications and features provided by 3PAR OS 3.2.2 MU3 and includes the following modifications:

Issue ID	Description
125219	Resolves a timing issue with iSCSI login in which the response was sent before iSCSI was aware of the new initiator.
135302	The system manager now frees space on a solid state drive (SSD) when it reaches 10% life left, instead of when it reaches 99%.
141510	Corrects an issue in which an unexpected controller node restart during node down lockstep can occur if the remote copy asynchronous group has been idle for an extended period.
144796	Corrects a memory handling issue that causes the <code>auth_helper</code> to end abnormally.
146519	Reduces potential memory usage during deduplication garbage collection process.
156705	Addresses an issue in which constrained memory resources in a 128-byte structure results in an unexpected controller node restart.
157865	Prevents unexpected controller node restarts due to transient errors reported to the Ethernet hardware driver.
158994	Resolves an issue that prevented iSCSI dynamic discovery completion during port provisioning sharing the same Send Target Port Tag.
159212	Resolves an issue that occurs when the last deduplication volume of a common provisioning group (CPG) is removed in the middle of an internal operation, such as region move or defragmentation task on the DDS, resulting in an orphaned deduplication store which is never cleaned and the space associated with the deduplication store is not released.
159311	Prevents a possible unexpected array restart due to a deadlock condition encountered during <code>ddscan</code> dry runs and virtual volume (VV) conversions.
160272	Improves cage firmware to prevent alerts indicating drives are "failed" when they are not.
161979	Improvements to ensure consistency in log page processing during fast commits used during node down recovery.

Table Continued

Issue ID	Description
163128	Removes unnecessary excessive logging of this SCSI message: "Request for Inq VPD page 0x8F/ECOP".
163902	Improves the task detail information of remote copy reverse task to identify remote copy reverse tasks that are not completed due to in-process region moves on any VV from a remote copy group.
163945	Prevents unexpected system manager restarts when moving regions between logical disks.
164689	Addresses a variable initialization to prevent a possible controller node restart when thin deduplicated virtual volumes (TDVVs) or related snapshots are removed.
165328	Refined the CPG free space limit alert. The alert now displays the correct CPG information when initiated. The alert is also cleared when the corrective action is taken.
166417	Corrects the setrcopygroup restore validation for asynchronous streaming remote copy which prevented the restore from being issued on a group that was stopped. A <code>setrcopygroup restore -nostart -nosync</code> command is now allowed for asynchronous streaming remote copy configurations.
167419	Corrects an issue where the array becomes unresponsive due to a thread holding a lock during the removal of peer motion source port that caused the system manager become unresponsive.
168992	Prevents a condition, if an array persistent port fails over and back quickly, where the fail back of the port may not succeed due to the Fibre Channel (FC) switch simultaneously detecting the WWN (Port Worldwide Name) on the failed over port and the original port.
169668	Improves the system manager cage management caching policy, allowing the system manager cage management code to better handle multiple client connections.
170003	Improves the performance of I/O on an iSCSI session when there are other connections logged in that are idle.
170017	Resolves an issue in which an inconsistent buffer type can lead to an unexpected controller node restart on the secondary array in a remote copy configuration.
170024	<code>cimserver</code> SMI-S API has been updated internally to reduce its memory consumption, which prevents unexpected controller node restarts, on systems where large numbers of active VLUNs and volumes are configured. Also corrects an issue which prevented <code>cimserver</code> from reporting all volume statistics under some situations.
170076	Reduces the impact of cleaning spare chunklets on SSDs, which resulted in performance issues, by reducing the rate of cleaning, as well as the priority of the SCSI command used to clean the chunklets.
170835	Corrects an issue wherein the collection of the power logs as part of the InSplore process caused Enclosure Management (NEMOE) to stop servicing the watchdog, which resulted in unnecessary customer alerts.

Table Continued

Issue ID	Description
178031	Corrects an issue in which an unused SAS port incorrectly shows as present.
178455	Corrects port concurrency issues by adding a reference counter to 16 Gb FC port structure.
180042	Avoids an unexpected array restart resulting from <code>updatevv</code> running against multiple VVs in succession.
180194	Prevents a controller node restart that results from a race condition when dropping the admin volume in the middle of snapshot removal.
180488	Resolves an unexpected controller node restart when <code>SCSI COMPARE_AND_WRITE</code> commands do not complete properly and there is an outstanding remote copy asynchronous streaming I/O request.
181203	Addresses an unexpected array restart resulting from an iSCSI <code>sendtarget</code> request from a host to the CNA card during online upgrades.
181429	Resolves an issue that leads to an unexpected controller node restart due to insufficient cleanup during port conversion from peer port to remote copy FC port.
181431	Resolves an issue in the NPORT ID change cleanup logic that resulted in an unexpected controller node restart.
181451	The System Reporter now uses cached values for drive temperature and SSD wear level. This approach saves considerable time while collecting data on systems with large numbers of drives.
182102	The 8 Gb FC adapter now responds to an out of order frame sequence, improving host I/O processing.
182164	Corrects the behavior of raw space alerts to be consistent between 3PAR OS versions. The raw space alert is now generated as expected based on the system parameter settings.
182704	Resolves an issue in which, after an offline upgrade, an array using encrypted drives and an external key manager (EKM) will not form a cluster.
183366	Resolves an unexpected controller node restart in remote copy asynchronous streaming configurations when a long period of time passes between replication cycles.
184112	Resolves an issue on 3PAR arrays with a small number of physical disks (PDs), where all the capacity is used, a RAID rebuild will now complete when a PD is marked "failed". This will now allow a <code>servicemag</code> operation to complete successfully.
184878	Corrects an issue in which log page allocation does not occur after processing a deduplication request and only when the volume is in write-through mode.
185358	Prevents controller node restarts by correctly clearing low pin count (LPC) bus alerts in the correctable advance error reporting (AER) range.

Table Continued

Issue ID	Description
185535	Addresses snapshot removal state issue between system manager and the kernel when a system manager restart occurs.
186754	Addresses an issue that occurs when attaining the status of the controller node drives, causing the integration process to stall.
187088	Improves log page list generation to maintain consistency. Also improves log page entry processing during node down recovery which is used during controller node restarts.
187158	Addresses an abort timeout issue which resulted in the hard reset of ports.

Known Issues with the OS

Issue ID	Description
146805	Remote copy data can become inconsistent if the secondary system runs out of space during a resynchronization, followed by a <code>stopcopygroup <rcgroup></code> before the resynchronization finishes if the remote copy group is then restarted.
167576	<code>Admithw</code> reconfigures all free FC ports to host/point and does not make a port type distinction. As a result, a remote copy FC port that was temporary free, for instance, during an upgrade procedure, could eventually be reconfigured as the host/point, causing outages.
174251	VMware hosts may disconnect from the 3PAR array if they are utilizing TDVVs and those volumes are converting from TDVV to thin provisioned virtual volumes (TPVVs).
178179	In an iSCSI configuration, if duplicate iSCSI Qualified Names (IQNs) are encountered, this may result in an unexpected controller node restart.
181445	Inaccessibility to certain VVs could be extended when the <code>checkvv</code> doesn't automatically start the VVs. The workaround is to run <code>checkvv</code> manually.
186317	A controller node restart may occur as a result of an excess number of initiators being zoned to FC ports. Limited zoning is required to avoid this issue.
188673	There can be a large, unused space overhead when small, fully provisioned CPVVs are rebalanced. This increases with larger RAID set sizes. Because of this, <code>tunesys</code> will not tune small volumes to prevent unnecessary space utilization.

3PAR OS Patches Included in this Release

This list includes all 3PAR OS patches included in this release since the last base maintenance update. To obtain copies of the patch release notes documents, go to the Hewlett Packard Enterprise Support Center.

- 3PAR OS 3.2.2 EGA Patch 35
- 3PAR OS 3.2.2 EGA Patch 43
- 3PAR OS 3.2.2 MU3 Patch 39
- 3PAR OS 3.2.2 MU3 Patch 41

- 3PAR OS 3.2.2 MU3 Patch 42
- 3PAR OS 3.2.2 MU3 Patch 45
- 3PAR OS 3.2.2 MU3 Patch 48
- 3PAR OS 3.2.1 MU3 Patch 45
- 3PAR OS 3.2.1 MU3 Patch 50

More information

<http://www.hpe.com/info/storage/docs/>
<http://www.hpe.com/support/hpesc>

What's New in the CLI

The following command options are added in 3PAR CLI 3.2.2 MU4:

- `settarget -rescan` now has `-force`.
- `createflashcache` maximum supported size is now up to 12 TiB.

Modifications to the CLI

Issue ID	Description
135718	Resolves an issue in which the output "Too many CLI connections" unexpectedly appeared when the SSMC was running for extended periods and connections would stall in the SSL handshake. <code>showuserconn</code> now shows these connections with a user as: <code>:authenticating:.</code>
168390	<code>checkhealth dar</code> now checks to ensure each admitted PD is in the <code>owned</code> or <code>fips_owned</code> state.
182892	Resolves a conflict between VV names starting with <code>wwn</code> and <code>wwn:<VV_WWN></code> syntax.

What's New with the CIM API Software

- The property `TPD_Fan.OperationalStatus` now reports "No Contact (12)" when a hot-swappable system fan is removed. Prior to this an empty `TPD_Fan` object was returned for the missing fan.
- The operation `ReplicationServices::ModifyReplicaSynchronization(resync)` now works for remote copy groups that are in the 3PAR Failover state of "Recovered". The `TPD_RemoteReplicationGroup` that corresponds to the remote copy group can now be "restored" with the SMI-S resync operation.
- `cimserver` now disables client authentication when HTTPS is enabled. In the past, `cimserver` enabled but did not support client authentication via HTTPS. This caused an issue for some `cimserver` clients.

What's New with the Web Services API Software

- Diffie Hellman key size for WSAPI port 8080 is now fixed at 2048 bits.
- Web Services API no longer returns an error if an array does not have the default password for the 3PAR admin user or if the 3PAR admin does not exist.
- Added a new "SmartSAN" license to the list of supported licenses returned by the following Web Services API call: `http(s)://<server_name>:<port>/api/v1/system`.

Verification

The installation of 3PAR OS 3.2.2 MU4 can be verified from an interactive CLI session by issuing the CLI command `showversion -a -b`.


```
cli% showversion -a -b
Release version 3.2.2.612 (MU4)
Patches: None

CLI Server 3.2.2.612 (MU4)
CLI Client 3.2.2.612
System Manager 3.2.2.612 (MU4)
Kernel 3.2.2.612 (MU4)
TPD Kernel Code 3.2.2.612 (MU4)
TPD Kernel Patch 3.2.2.612 (MU4)
CIM Server 3.2.2.612 (MU4)
WSAPI Server 3.2.2.612 (MU4)
Console Menu 3.2.2.612 (MU4)
Event Manager 3.2.2.612 (MU4)
Internal Test Tools 3.2.2.612 (MU4)
LD Check Tools 3.2.2.612 (MU4)
Network Controller 3.2.2.612 (MU4)
Node Disk Scrubber 3.2.2.612 (MU4)
PD Scrubber 3.2.2.612 (MU4)
Per-Node Server 3.2.2.612 (MU4)
Persistent Repository 3.2.2.612 (MU4)
Powerfail Tools 3.2.2.612 (MU4)
Preserved Data Tools 3.2.2.612 (MU4)
Process Monitor 3.2.2.612 (MU4)
Rolling Upgrade Tools 3.2.2.612 (MU4)
Software Updater 3.2.2.612 (MU4)
TOC Server 3.2.2.612 (MU4)
VV Check Tools 3.2.2.612 (MU4)
File Persona 1.2.2.6-20161017
SNMP Agent 1.8.0
SSH 6.6p1-4~bpo70+1
VASA Provider 2.2.10
Firmware Database 3.2.2.612 (MU4)
Drive Firmware 3.2.2.612 (MU4)
UEFI BIOS 04.08.38
MCU Firmware (OKI) 4.8.29
MCU Firmware (STM) 5.2.53
Cage Firmware (DC1) 4.44
Cage Firmware (DC2) 2.64
Cage Firmware (DC3) 08
Cage Firmware (DC4) 2.64
Cage Firmware (DCN1) 4078
Cage Firmware (DCN2) 4078
Cage Firmware (DCS1) 4078
Cage Firmware (DCS2) 4078
Cage Firmware (DCS5) 1.93
Cage Firmware (DCS6) 1.93
Cage Firmware (DCS7) 4078
Cage Firmware (DCS8) 4078
QLogic QLA4052C HBA Firmware 03.00.01.77
QLogic QLE8242 CNA Firmware 04.15.08
QLogic 8300 HBA FC Firmware 08.01.05
QLogic 8300 HBA FCoE Firmware 08.01.05
QLogic 8300 HBA iSCSI Firmware 05.07.06
```

Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x11
Emulex LPe12004 HBA Firmware	02.03.x11
Emulex LPe16002 HBA Firmware	10.6.248.4
Emulex LPe16004 HBA Firmware	10.6.248.4
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

3PAR OS 3.2.2 EMU4 Release Notes

Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 EMU4 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*. To obtain a copy of this documentation, go to <http://www.hpe.com/info/enterprise/docs>.

CAUTION:

- 3PAR 3.2.2 EGA Patch 35 must be installed prior to upgrading from 3PAR 3.2.2 EGA to a later version.
- 3PAR 3.2.2 MU1 Patch 37 must be installed prior to upgrading from 3PAR 3.2.2 MU1 to a later version.

Supported Platforms

For details of supported HPE 3PAR StoreServ Storage, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

More information

<http://www.hpe.com/storage/spock>

Components

Component	Version
OS	3.2.2.642 (P59)
CLI Client	3.2.2.642
SNMP Agent	1.8.0
File Persona	1.2.3.2-20161117 (P51)
Drive Cage Firmware:	
DC4 Firmware	2.64
MCU Firmware (OKI)	4.8.29
MCU Firmware (STM)	5.2.53
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	4078
DCS5 / DCS 6 Firmware	1.93

Table Continued

Component	Version
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.08
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.03.x11
Emulex LPe12004 HBA Firmware	02.03.x11
Emulex LPe16002 HBA Firmware	10.6.248.4
Emulex LPe16004 HBA Firmware	10.4.248.4
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.00.00

Modifications to the OS

3PAR OS 3.2.2 EMU4 combines all of the modifications and features provided by 3PAR OS 3.2.2 MU4 Patch 51, Patch 56, Patch 58, Patch 59, and Patch 73.

Refer to the release notes documents for each patch for a full list of modifications, features and supported drives. To learn more about each patch, use the links provided to access the individual patch release notes.

3PAR OS 3.2.2 MU4 Patch	Description	Obsoletes	Links to Documentation
Patch 51	P51 provides several important quality improvements for File Persona.	None	<u>HPE 3PAR OS 3.2.2 MU4 Patch 51 Release Notes</u>
Patch 56	Patch 56 provides several quality improvements in volume management, DIF handling, and remote copy.	OS-3.2.2.61 2-P54	<u>HPE 3PAR OS 3.2.2 MU4 Patch 56 Release Notes</u>

Table Continued

3PAR OS 3.2.2 MU4 Patch	Description	Obsoletes	Links to Documentation
Patch 58	Patch 58 provides support for drive FW updates and new drives	None	<u>HPE 3PAR OS 3.2.2 MU4 Patch 58 Release Notes</u>
Patch 59	Patch 59 provides several quality and supportability improvements	None	<u>HPE 3PAR OS 3.2.2 MU4 Patch 59 Release Notes</u>
Patch 73	Patch 73 provides support for drive FW updates and new drives	OS-3.2.2.61 2-P72	<u>HPE 3PAR OS 3.2.2 MU4 Patch 73 Release Notes</u>

3PAR OS 3.2.2 EMU4 also includes the following modification:

Provides embedded support for new controller node boot drives. This allows seamless upgrades from previous HPE 3PAR OS 3.2.2 versions where new controller node drives are installed either through a hardware upgrade or by maintenance where the Field Replaceable Unit (FRU) is a new controller node boot drive.

3PAR OS 3.2.2 MU6 Release Notes

OS Online Upgrade Considerations

This feature allows upgrade of the OS concurrently with I/O activity on the attached hosts, provided certain conditions are met. For more information regarding the required order for upgrade and installation of software components, see the *HPE 3PAR OS 3.2.2 MU6 Upgrade Instructions*. For further information and pre-planning of online upgrades, refer to the latest version of the *HPE 3PAR OS Upgrade Pre-Planning Guide*.

All the content from previous 3.2.2 maintenance updates are included in 3PAR OS 3.2.2 MU6. For a list of patches included in this maintenance update, see **3PAR OS Patches Included in this Release**.

Warnings, Cautions and Notes

CAUTION:

It is highly recommended that the array has all available patches applied before beginning the upgrade to 3.2.2 MU6.

Supported Platforms

For details of supported HPE 3PAR StoreServ Storage, see the Single Point of Connectivity Knowledge (SPOCK) website at <http://www.hpe.com/storage/spock>.

More information

<http://www.hpe.com/storage/spock>

Components Included in 3PAR OS 3.2.2 MU6

Component	Version
CLI Server	3.2.2.709 (MU6)
CLI Client	3.2.2.709
System Manager	3.2.2.709 (MU6)
Kernel	3.2.2.709 (MU6)
TPD Kernel Code	3.2.2.709 (MU6)
CIM Server	3.2.2.709 (MU6)
WSAPI Server	3.2.2.709 (MU6)
Console Menu	3.2.2.709 (MU6)
Event Manager	3.2.2.709 (MU6)

Table Continued

Component	Version
Internal Test Tools	3.2.2.709 (MU6)
LD Check Tools	3.2.2.709 (MU6)
Network Controller	3.2.2.709 (MU6)
Node Disk Scrubber	3.2.2.709 (MU6)
PD Scrubber	3.2.2.709 (MU6)
Per-Node Server	3.2.2.709 (MU6)
Persistent Repository	3.2.2.709 (MU6)
Powerfail Tools	3.2.2.709 (MU6)
Preserved Data Tools	3.2.2.709 (MU6)
Process Monitor	3.2.2.709 (MU6)
Rolling Upgrade Tools	3.2.2.709 (MU6)
Software Updater	3.2.2.709 (MU6)
TOC Server	3.2.2.709 (MU6)
VV Check Tools	3.2.2.709 (MU6)
SNMP Agent	1.8.0
File Persona	1.2.4.3-20170601
SSH	6.6p1-4~bpo70+1
VASA Provider	2.2.10
Firmware Database	3.2.2.709 (MU6)
Drive Firmware	3.2.2.709 (MU6)
UEFI BIOS	04.08.39
Drive Cage Firmware:	
MCU Firmware (OKI)	4.8.29
MCU Firmware (STM)	5.2.53
DC1 Firmware	4.44

Table Continued

Component	Version
DC2 / DC4 Firmware	2.64
DC3	08
DCN1 / DCN2 / DCS1 / DCS2 /DCS7 / DCS8 Firmware	4078
DCS5 / DCS6 Firmware	2.86
HBA Firmware:	
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.08
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.06
Emulex LP11002 HBA Firmware	02.10.x03
Emulex LPe12002 HBA Firmware	02.10.x03
Emulex LPe12004 HBA Firmware	02.03.x11
Emulex LPe16002 HBA Firmware	10.6.248.4
Emulex LPe16004 HBA Firmware	10.6.248.4
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.10.01

What's New in the OS

This section describes all the new features introduced in the 322 MU6 release:

- Updates to enhance HPE 3PAR OS security.
- Enhances HPE 3PAR StoreServ 20000 drive cage firmware.
- Enhancements with online conversions, online copy, online promote, `updatevv`, and imports exhibiting long I/O stall times on HPE StoreServ 20000 systems due to internal structure invalidation.
- Improvement in the host I/O stall times near the end of a Peer Motion migration where consistency groups are used.

- Improvement in the host I/O stall times while processing `updatevv` of VV sets and while importing consistency groups.
- Resolution to the issue where the cache server (cachesvr) was unexpectedly restarting while an `updatevv` was in progress where there were snapshots present.
- Added support for the following cables:
QSFP+ 4x10G SFP+ 3m DAC cables (HPE PN JH659A)

Manufacturer	Part Number
Arista Networks	CAB-Q-S-3M
USCRITICAL	QSFP-4X10G-AOC5M
Fiberstore	QSFP-4SFP10G-DAC
CISCO-AVAGO	AFBR-7IER05Z-CS1

Modifications to the OS

3PAR OS 3.2.2 MU6 includes the following modifications:

Issue ID	Description
109762	Prevents an issue where a controller node may reintegrate into the array too quickly after the controller node restarts.
138977	Prevents an unexpected controller node restart when a SCSI request time out occurs.
141238	Increased the number of pre-allocated memory elements to accommodate higher I/O workloads.
142459	Prevents an unexpected controller node restart when removing a virtual volume that has outstanding requests.
165155	Corrects an unexpected System Manager restart when a VV is updated to a group target that is not yet established in 3-way Peer Persistence configurations.
168654	Prevents an unexpected controller node restart when snapshot volumes are being removed from an array with limited free space.
169024	Flash cache is removed from the array if the meta data creation does not succeed on the controller node during controller node integration processing.
170080	Prevents setting expiration times for volumes or snapshots not manually created in a Remote Copy (RC) group.
170293	Synchronizes snapshot removal operations between all controller nodes if a controller node is restarted while the snapshot is being deleted.

Table Continued

Issue ID	Description
175541	Prevents long execution times on CPUs while servicing extended copy operations, avoiding an unexpected array restart due to missing cluster heartbeats.
178400	Reduces the amount of SCSI Command Transport messages logged.
179732	Corrects the issue where the dirty pages were not flushed during snapshot removal causing timeouts which may lead to an unexpected array restart.
180613	After an unexpected array restart, the System Manager is not automatically starting which prevents the controller nodes from integrating into the cluster.
181445	Prevents the <code>checkvv</code> command from running a second full volume check before the volume is online and available when a check has already completed for that volume.
182704	Resolves an issue where, after an offline upgrade, an encrypted array using an External Key Manager (EKM) would not form a cluster.
182808	Prevents an unexpected controller node restart when using v-ports.
183278	Resolves an issue where the event log was flooded with CLI login events from the System Reporter.
185303	Corrects an issue where the defragmentation of the DDS was performing too slowly not allowing defragmentation to complete.
185780	Prevents an issue where there was an unexpected SAS HBA restart due to a cache correctable error.
186317	Resolves an unexpected controller node restart due to the HBA driver allowing more than the maximum number of initiators on the port.
186732	Prevents an unexpected Converged Network Adapter (CNA) firmware restart triggered by mailbox commands not completing in a timely manner.
188750	Prevents HBA LPe16004B firmware restarts resulting from the firmware not clearing certain interrupts.
188778	Corrects an issue during the HPE 3PAR OS upgrade process where a portion of the file system was not mounted correctly.
188839	Corrects an issue where a host loses access to its Virtual Volumes (VV) when the host is removed from the secondary RC group and added to a primary RC group.
189061	Added an alert to warn of potential misconfiguration of the host connection.
190904	Prevents unnecessary restart of the System Manager.
191019	Limit the number of retries and increase the delay between retries that the Fibre Channel HBA can attempt to log into a FC switch port.

Table Continued

Issue ID	Description
191212	When restarting the System Manager on an array using persistent ports, the System Manager application may terminate unexpectedly.
192531	Removes the requirement for the Common Name to be specified in certificates. This prevented certificate authentication from working on a valid certificate.
193352	Corrects the behavior that creates a high volume of false "fixed" alerts that is triggered by the controller node drive health check which is performed on a routine basis.
194886	Prevents a condition that arises from a temporary loss of drive cage power whereby some Physical Disks (PDs) have chunklets within the same RAID set marked stale causing the Virtual Volume (VV) to be marked preserved.
195084	Corrects an issue where the <code>tunevv</code> operation was using an inaccurate growth size calculation preventing the overall tune operation to complete successfully.
195611	Places secondary volumes in standby state when a Peer Persistence fail-over is interrupted.
196169	In Peer Motion configurations, a high volume of events are no longer logged due to the periodic Physical Disk (PD) health check.
196653	After upgrading the HPE 3PAR OS, SSD drives with the 100 RPM designation have a chunklet failure threshold that is exceeded due to differences in failed chunklet calculations between HPE 3PAR OS versions.
196954	Prevents host path loss during switch firmware update.
197102	Prevents an unexpected controller node restart when using Thinly Deduplicated Virtual Volumes (TDVV).
197853	Addresses an issue where, in certain SAN configurations, the CLI command <code>showportdev</code> was not returning any output.
197114	Prevents unexpected LPe16004B HBA restarts due to a parity issue.
198437	Resolves an issue where long I/O pauses were experienced by an ESX host during controller node recovery failback operations.
198548	Resolved an issue where a cli-lib message was filling the System Manager log with debug messages.
199872	Prevents new volumes from being created in the CPG with <code>-ha mag</code> when <code>-ha mag</code> is requested.
199964	Improved initial synchronization and re-synchronization of Remote Copy groups to not impact Remote Copy heartbeat detection.
200023	Corrects an issue where the <code>showpatch -hist</code> command was displaying "NA" instead of the correct identifier.

Table Continued

Issue ID	Description
200073	Resolves the condition that when adding a Virtual Volume (VV) to a vvset with a Quality of Service (QoS) rule defined, the VV will maintain the default QoS Rule.
202480	Prevents an Asynchronous Logical Unit Access (ALUA) transition on Synchronous Remote Copy groups while the groups are in a stopped state.
202630	Corrects an issue that truncated valuable diagnostic information because the logging was too verbose.
202808	Resolves the situation of background drive operations occurring at the same time as an encryption operation where the encryption operation may not complete preventing the controller nodes from joining the cluster.
202836	Resolves an issue where VMware ESX host could not mount 3PAR iSCSI VLUNS when jumbo frames were enabled.
203090	Resolved an issue during an on-line HPE 3PAR OS upgrade that the controller node reboot may not complete due to an HBA port being in maintenance mode.
204455	Prevents VLUNS from being exported to hosts on HBA ports which are defined as Remote Copy Fibre Channel (RCFC) ports.
204987	Resolved an issue where array host ports were unable to log into the SAN fabric after receiving abort messages from the hosts.
205515	Resolved an issue where a <code>servicemag</code> operation will not complete and reports a duplicate chunklet destination.
205678	Prevents an unexpected controller node restart when hosts are configured to use Offloaded Data Transfer (ODX)..
205786	Addresses a timing issue during a controller node down or an HPE 3PAR OS upgrade scenario when the required metadata is not yet available.
206128	Prevents configuring more than 2 Peer Motion ports per controller node pair.
208350	Prevents the authorization service on the array from consuming the controller node CPU when LDAP binding is unsuccessful using Simple Authentication & Security Layer (SASL).
210121	Resolved an issue calculating the maximum I/O queue depth on host ports.
211978	Resolves a soft reset on the array's host port LPe12004 HBA.
207559	Prevents physical copy writes to system volumes.
211011	Prevents the CLI from becoming unresponsive while performing an <code>updatevv</code> on a vvset with a large number of VV in the vvset.
213997	Improved dual boot drive error handling for StoreServ 20000.

Table Continued

Issue ID	Description
214447	Resolves an issue with memory management when a Fibre Channel over Ethernet (FCoE) port cannot log in.
214448	Improved performance of snapshot removal when multiple snapshots are present or removed.
215044	Prevents a given Virtual Volume (VV) from being exported more than once to a host.
215433	Enables Service Processor (SP) to remain connected to the StoreServ when non-encrypted network ports are disabled on the array.
215766	Corrects an issue where the array's internal table data backup mechanism is overextended which can lead to the array becoming administratively unresponsive and, in very extreme situations, could lead to data becoming unavailable.
215894	Snapshot removal or space reclamation on a Thinly Provisioned Virtual Volume (TPVV) causes internal logging issues which leads to unexpected controller node restarts.
217036	Resolved the condition of a false disk slot temperature alert when certain SSD models were installed in StoreServ 20000 arrays.

Known Issues with the OS

Issue ID	Description	Workaround
200537	After a controlled failover operation on Remote Copy with Peer Persistence configured, if a Virtual Volume (VV) is dismissed from the secondary remote copy group, and then is admitted to a new remote copy group and exported to a host, both arrays will assign the Target Port Group ID (TPGID) of 258 to the VV and the hosts will be unable to access the VV.	Use the CLI command <code>setvv -settpgid 257 <vvname></code> and then admit the VV to the Remote Copy group.
205700	The slow disk checker may not identify a disk as slow and remove it from the system, if there are no other active disks to compare it with.	Identify the disk with high queue length of long service times, and eject it from the system with the established procedures.
213823	The ddcscan task in dryrun may report a negative value for CRC used, indicating negative amount of space to be freed.	None. This is a background system task running in dryrun, not reporting the correct estimate of the space to be freed.
219232	By feature design, Interrupt Coalescence is not supported and is not used in HPE 3PAR OS for 16Gb FC adapter/driver on StoreServ arrays.	None.

3PAR OS Patches Included in this Release

This list includes all 3PAR OS patches included in this release since the last base maintenance update. To obtain copies of the patch release notes documents, go to the Hewlett Packard Enterprise Support Center.

Patch Name	Link to the Patch
HPE 3PAR OS 3.2.2 MU4 Patch 84	<u>HPE 3PAR OS 3.2.2 MU4 Patch 84</u>
HPE 3PAR OS 3.2.2 MU4 Patch 85	<u>HPE 3PAR OS 3.2.2 MU4 Patch 85</u>
HPE 3PAR OS 3.2.2 MU4 Patch 91	<u>HPE 3PAR OS 3.2.2 MU4 Patch 91</u>
HPE 3PAR OS 3.2.2 MU4 Patch 92	<u>HPE 3PAR OS 3.2.2 MU4 Patch 92</u>

Modifications to the CLI

Issue ID	Description
140159	The <code>checkhealth</code> command reports unqualified SAS backend cables on StoreServ 8000 and StoreServ 20000.
169795	Resolves an unexpected termination of the <code>tunesys</code> command when low freespace conditions exist if small volumes are present.
192194	Prevents <code>tuneld</code> from being run by users from the Service and Browse user permission groups.
193846	Resolved an issue where custom options for <code>tunesys</code> were not used when acting on active-active PDs.
196065	Corrects an issue with <code>tunesys</code> where the total used size of the Virtual Volume was inaccurately calculated causing the <code>tunesys</code> to skip certain volumes.

Changed Commands

The following command options were changed in the 3PAR 3.2.2 MU6 CLI :

Command	Options added (unless stated otherwise)
<code>setsys</code>	<code>SingleLunHost</code>

What's New with the CIM API Software

The following additions are new in the CIM API Software features with the 322 MU6 release:

- An informative message indicating an expected `pr_read_value_table()` read error is no longer written to the `syslog` message log.
- Caches data such that frequent CIM server API calls by 3rd party software that retrieve manufacturing information for cages, magazines, and nodes won't result in invalid error messages and events being logged because the internal interface is busy.
- Corrects an issue whereby CIM server would occasionally deadlock during its process shutdown, such as when a patch is installed. When this occurs the `em_filter` process that forwards notifications would also eventually stall. Tools like WSAPI and SSMC and any 3rd party software would not receive event notifications.

Verification

The installation of 3PAR OS 3.2.2 MU6 can be verified from an interactive CLI session by issuing the CLI command `showversion -a -b`.

```
cli% showversion -a -b
Release version 3.2.2.709 (MU6)
Patches: None
```

Component Name	Version
CLI Server	3.2.2.709 (MU6)
CLI Client	3.2.2.709
System Manager	3.2.2.709 (MU6)
Kernel	3.2.2.709 (MU6)
TPD Kernel Code	3.2.2.709 (MU6)
CIM Server	3.2.2.709 (MU6)
WSAPI Server	3.2.2.709 (MU6)
Console Menu	3.2.2.709 (MU6)
Event Manager	3.2.2.709 (MU6)
Internal Test Tools	3.2.2.709 (MU6)
LD Check Tools	3.2.2.709 (MU6)
Network Controller	3.2.2.709 (MU6)
Node Disk Scrubber	3.2.2.709 (MU6)
PD Scrubber	3.2.2.709 (MU6)
Per-Node Server	3.2.2.709 (MU6)
Persistent Repository	3.2.2.709 (MU6)
Powerfail Tools	3.2.2.709 (MU6)
Preserved Data Tools	3.2.2.709 (MU6)
Process Monitor	3.2.2.709 (MU6)
Rolling Upgrade Tools	3.2.2.709 (MU6)
Software Updater	3.2.2.709 (MU6)
TOC Server	3.2.2.709 (MU6)
VV Check Tools	3.2.2.709 (MU6)
File Persona	1.2.4.3-20170601
SNMP Agent	1.8.0
SSH	6.6p1-4~bpo70+1
VASA Provider	2.2.10
Firmware Database	3.2.2.709 (MU6)
Drive Firmware	3.2.2.709 (MU6)
UEFI BIOS	04.08.39
MCU Firmware (OKI)	4.8.29
MCU Firmware (STM)	5.2.53
Cage Firmware (DC1)	4.44
Cage Firmware (DC2)	2.64
Cage Firmware (DC3)	08
Cage Firmware (DC4)	2.64
Cage Firmware (DCN1)	4078
Cage Firmware (DCN2)	4078
Cage Firmware (DCS1)	4078
Cage Firmware (DCS2)	4078
Cage Firmware (DCS5)	2.86
Cage Firmware (DCS6)	2.86
Cage Firmware (DCS7)	4078
Cage Firmware (DCS8)	4078
QLogic QLA4052C HBA Firmware	03.00.01.77
QLogic QLE8242 CNA Firmware	04.15.08
QLogic 8300 HBA FC Firmware	08.01.05
QLogic 8300 HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.07

Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.10.x03
Emulex LPe12004 HBA Firmware	02.10.x03
Emulex LPe16002 HBA Firmware	10.6.248.8
Emulex LPe16004 HBA Firmware	10.6.248.8
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.00
LSI 9205-8e HBA Firmware	17.11.00
LSI 9300-8e HBA Firmware	07.10.01

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website: www.hpe.com/assistance
- To access documentation and support services, go to the HP Support Center – Hewlett Packard Enterprise website: www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:

- HP Support Center – Hewlett Packard Enterprise

Get connected with updates from HP

page: www.hpe.com/support/e-updates

- Software Depot website: www.hpe.com/support/softwaredepot

- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the HP Support Center – Hewlett Packard Enterprise

More Information on Access to HP Support Materials

page: www.hpe.com/support/AccessToSupportMaterials

**IMPORTANT:**

Access to some updates might require product entitlement when accessed through the HP Support Center – Hewlett Packard Enterprise. You must have a Hewlett Packard Enterprise Passport set up with relevant entitlements.

Websites

Website	Link
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair	www.hpe.com/support/selfrepair
Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix	www.hpe.com/storage/spock
Storage white papers and analyst reports	www.hpe.com/storage/whitepapers

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback

(docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.